Conclusions of civil society and public sector policy discussions on data use in government

Contents

This document is a summary of civil society and public sector policy discussions on data uses in government. This document captures the discussions that have taken place. In circulating this document we are not seeking to open up new issues or re-open issues that have already been discussed.

Introduction

1. Since March 2014 civil society organisations, privacy groups, officials from a number of government departments, academics and representatives from parts of the wider public sector have been collectively discussing how government can be made to be more efficient and effective through its use of data. The core focus has been to enhance the availability of high quality research and statistics from administrative data; prevent fraud and help citizens manage the debt they have with government; and ensure the right services are offered to the right person at the right time. The findings set out in this document do not represent the views of HM Government (HMG) but summarise the conclusions of those individuals who participated in discussions. Given the large range of people and organisations involved, the findings and recommendations set out in this paper are important and will inform future work in the area, which may involve further consultation.

2. Work on this policy initially began using conventional Whitehall policy development approaches, with a focus and presumption that data sharing offered the solution to its objectives. However, it became apparent that determining where the balance between the proportionate use of data to deliver services and maintaining people's privacy would be a sensitive and difficult exercise to do in isolation, particularly because of the variable levels of citizens' trust of government on the subject of data[1]. An open policy making (OPM) approach was adopted to ensure there was a shared understanding of both what government wanted to achieve and the concerns of those outside of government.

3. Involve, a not for profit organisation established to improve public engagement with government, were asked by the Cabinet Office to work collaboratively on an open policy making process on this issue. Involve agreed to help facilitate the process and external engagement. Since then over two hundred organisations have been invited to participate based on their particular interest in the issues considered. The OPM process has been open to any interested organisations to join. The number of non-government individuals and organisations willing and able to participate in the process was fewer than anticipated. Resourcing issues, particularly where the organisation is relatively small, has been a key factor. Groups engaged in the process included those with a specific interest in individual privacy and rights, academics, statisticians, researchers and their funders, charities, government officials and some private sector organisations.

---

[1] Sciencewise (2014) Big data: Public views on the collection, use and sharing of personal data by government and companies - http://www.sciencewise-erc.org.uk/cms/public-views-on-big-data/

Representatives from these organisations and individuals participated in discussions and the development of proposals in each of the themes. The scope of this new joint work was expanded to include looking at alternative solutions, not just data sharing. The task set was to examine the evidence and use the analysis to inform the design of policy proposals from it. The process was designed to ensure that all voices were heard from the outset, increasing the likelihood of balanced, successful policy recommendations being delivered.

4. Transparency has underpinned the whole process, with all work as open as possible. Key information and updates have been posted on www.datasharing.org.uk, a non-government website, to act as a repository and audit trail of the work.

5. The following key principles have underpinned the discussions:

    a. Proposals should **not** consider the building of new large and permanent databases, or collecting more data on citizens;
    b. Proposals should **avoid** the indiscriminate sharing of data within Government; and
    c. Proposals should **not** weaken the Data Protection Act.

6. The findings set out in this paper offer a balanced consideration of options by the individuals involved, including more data sharing as a potential solution to the specific challenges we looked at. It is the product of a truly open collaboration between a range of public sector officials and civil society organisations and privacy campaigners. In some instances, the consensus among the group was that legislative changes along with appropriate safeguards would be the best course of action to achieve the objectives. Whilst with other issues, the consensus was that data sharing was not the best solution. These balanced recommendations demonstrate the value of the open policy making approach and collaborating with a range of organisations with different perspectives.

7. There remain some areas, particularly around safeguards that will need to be in place where data is to be shared, where further and wider consultation is required, as consensus could not be achieved. Government would wish to consult further on the full range of policy proposals before deciding which to take forward and in what exact form.

8. Cabinet Office is engaging with officials from devolved administrations in Wales, Scotland and Northern Ireland to determine the cross-border implications of the proposals and to consider whether there would be scope or demand for some of

the policies to apply in devolved nations either identically or with particular differences. Devolution issues are complex because of the differing areas of competence in the settlements and differing functions of bodies working in devolved areas. We will consider findings as they emerge and identify where there is scope for cooperation to achieve agreed outcomes across different parts of the UK.

9. Open policy making still represents a new way of working. Taking this approach to an issue as challenging as data sharing builds on the excellent work delivered by using this approach to develop the UK's 2013-15 Open Government Partnership national action plan. This process provides further evidence of the value of working in partnership to look at some of our biggest challenges.

Summary

10. The OPM process has been extensive, with engagement taking place at individual and group levels, either for individual specific policy challenges or across the policy areas. Over twenty sessions were run with a large number of representatives between April and the end of 2014. Representatives from both within and outside government have listened and changed their position where the case has been compelling. To ensure transparency, all key discussion documents were posted on www.datasharing.org.uk, a non-government website, and invited comments from the general public.

11. The following three specific policy challenges were explored as part of the open policy making process:

- Research and statistics – improving the quality of statistics and enabling the availability of better evidence to inform the formulation of policy and delivery decisions;
- Fraud, error and debt – saving taxpayer's money wasted on fraud and error and provide those citizens with multiple debts to government greater support to help manage their debts; and
- Tailored public services – improving the tailoring of public services so that the right services are offered and provided to the right person at the right time.

12. A brief summary of the OPM group's key recommendations are:

Research and statistics

De-identified data

- Representatives from both within and outside government recognised the need for public bodies to be able to link data for research purposes. Representatives were supportive of a proposal, provided data linking was carried out using a Trusted Third Party sharing system. This process uses significant procedures to de-identify data so that it can be linked in a secure access facility and made available to researchers under controlled conditions. Trusted Third Parties, researchers, and the subject of the research would all have to be accredited by an accreditation body under a system established through legislation. Any research intended to make use of this system under the legislation would have to satisfy the specified condition that the research 'is in the public interest'. Extensive consultation via the open policy making process led to consensus on the aims and proposed powers. It was proposed that specifically defined health services and social care bodies would be excluded from these proposed new powers.

Identified data

- Participants in the open policy making process considered a specific proposal from Government to enable public authorities to disclose data to the Office for National Statistics (ONS) in order to allow it to carry out the executive functions of the UK Statistics Authority (Authority) to provide statistics that serve the public good. The proposal would replace the current arrangements whereby the Minister for the Cabinet Office provides an information gateway through regulations, which are approved by Parliament through affirmative resolution process. This would reduce the burden on businesses and other respondents by reducing the cost of surveys as well as time taken by respondents to complete them; improve policy making decisions based on research and statistics by strengthening the evidence base for policies; improve the quality of statistics, while preserving the privacy of data subjects and ensuring that data are used appropriately, by ensuring that safeguards are embedded in the process. It was agreed that changes to legislation would be required to meet the identified objectives.

- The group identified alternative options for the scrutiny of proposals for disclosure of administrative identified data to ONS, with advantages and disadvantages, but there was no consensus on any of the options. There have been strong representations from some elements of Civil Society that the Parliamentary process described above for opening new gateways should be sacrosanct.

HM Revenue and Customs (HMRC) general and aggregated and de-identified data

- Participants in the open policy making process agreed with a Government proposal to reduce the restrictions around the disclosure of less sensitive general, aggregated and individual level de-identified HMRC data for public benefit. Legislation limits the circumstances in which HMRC may share information. Most other central government departments are not subject to equivalent restrictions, and thus this proposal helps achieve greater equality for HMRC, enabling it to contribute to a wider range of government initiatives and academic research projects than at present. Representatives from within and outside government agreed with the aims and the rationale for legislative change. HMRC has already consulted on this proposal.

Fraud, error and debt

- Representatives from both within and outside government called for more robust evidence to be gathered on a range of fraud, error and debt issues (from the scale of the problem to the value of different types of intervention) from which assessments of potential options could be made.

- It was agreed that a set of pilots be developed, some requiring new legislation, to explore the value of interventions through data sharing. Pilots

would include feedback mechanisms to provide insight into the demand for data sharing, and citizen attitudes to data use to counter fraud.

- Consensus between participants was that it may be difficult to determine a clear line between fraud and error, making any work that specifies error separate to fraud potentially uncertain and therefore less likely to be successful. It was also agreed that non-legislative avenues may be able to address error. Further, it is likely that an amount of error will be reduced through the increased data quality that work to reduce fraud would help to deliver.

- OPM Group participants agreed that there are benefits to the debtor from a reduced number of approaches and a combined management of debt. The Debt Market Integrator (DMI)[2] work will provide a single point of access to a wide range of debt management and collection services. Later developments could include a single view of debt and supports debtors through the development of a single payment plan. Whilst some preferred a legislative approach, the group were keen that a consent-based approach be tried first. This consent-based approach would be reviewed and a decision would be made as to whether it continues or whether more formal intervention is required. To manage the risk of wasted revenue due to delay should this process be necessary, the group have proposed that parallel preparatory work on legislation should be carried out whilst the consent-based work is assessed.

Tailored public services

- Participants in the OPM process agreed that there was value in exploring data sharing to support the delivery of public services better tailored to individual need.

- The initial proposal was for specific gateways to address specific issues. Through an iterative policy development process, which explored a range of social policy areas, the group have developed and reached agreement on recommending a broader but constrained power. This would be a permissive power for *defined public bodies* to share data with *defined public bodies* for the purposes of improving the delivery or targeting of public services, in specified areas of social policy, resulting in an offer of help to an individual. Examples of specific objectives which would meet the criteria for the power, or not, are detailed below.

---

2 A cross-government project to consolidate and tackle outstanding government debts using a Debt Market Integrator (a joint public-private sector organisation) to provide access to a wide range of private sector debt collection services and suppliers.

- This power would be intended to operate in accordance with a number of principles:
    - The intent of the power is to help individuals by endeavouring to ensure that they are offered the right intervention at the right time.
    - The purpose of the data sharing would be to benefit individuals, not to punish them or do anything to their detriment.
    - Data matched but not used for the purpose described in the business case would be disposed of according to relevant information governance processes and not used for any other purpose.
    - The business case (for the specific data share) includes – under the objective - *details of the intervention that will enable the achievement of the objective*.

- Furthermore, discussions around the specified bodies that would be designated resulted in restricting these to public bodies. It was felt that this would result in significant improvement in the delivery of services to citizens while protecting citizen data.

<u>Safeguards</u>

- Throughout this process we have considered and challenged whether data sharing and legislative solutions are required to achieve the desired outcomes or whether other approaches could be taken. We believe these recommendations reflect this approach. They adhere to our principles that we would not develop solutions which require the building of large permanent databases or collecting more data on citizens, or weaken the protections afforded by the Data Protection Act.

- Where a solution, which requires changes to data sharing legislation, has been recommended, it is supported by measures that provide appropriate safeguards to protect the privacy of citizens. The need to be transparent has been at the core of the discussions and as a result options include making privacy impact assessments available for public scrutiny. In developing these proposals we have sought to balance a consistent approach across the different areas with the necessary tailoring to ensure that the unique features of each area are addressed appropriately, informed by the broader framework within which they fit. This has led to a few key differences in approach being taken across the three strands.

Part 1 – Why are we doing this?

13. Technology has transformed many aspects of our lives. Private and public sector technology enabled services such as online banking, shopping, renewing road fund licences for vehicles and registering to vote have improved the convenience and speed of the way citizens receive services and as a result expectations have increased. Though technology has enabled significant improvements to the delivery of public services, in some instances the citizen experience of public services may be poor. Citizens are often asked to complete and submit different forms and receive contact from different agencies with little evidence of coordination between public agencies. The experience can be confusing and at times it is difficult to understand what is available by way of public services. Furthermore, some of the most vulnerable citizens are not identified or contacted with the offer of support because of the inability of those delivering public services to work effectively together.

14. Though the foundations of the UK's economic recovery have been laid, the structural deficit remains and we will continue to live in a time of spending constraint. Citizens understand that public bodies are working within tight spending constraints and expect a continued drive to reduce waste and find the most efficient way of delivering public services in a way relevant to the world around all of us. Advances in technology allow organisations the ability to link and process large amounts of data to provide insights, which enable the delivery of better and more efficient services, thereby balancing these two challenges.

15. Accurate and timely data underpins the delivery of many of the modern services we receive whether public or private. Good data are critical to help inform the decisions made by government throughout the lifecycle of public service delivery. It plays a critical role in determining the services that are developed and offered to citizens. Population statistics and other data provide the evidence, which skilled analysts and policy officials use to inform the policy formulation process and appraisal of options. Data are also used to inform the key operational decisions that ensure the right services are offered and delivered to the right citizens at the right time. They can also be used to reduce waste such as instances where multi-agency cooperation can help identify when taxpayer's money is lost through fraud as well as reduce duplication of investigative and administrative functions across agencies.

16. A good example of what can be achieved by way of effective data sharing to deliver an outcome with a public benefit is the recent work by the Cabinet Office

and the Department for Work and Pensions (DWP) on Individual Electoral Registration (IER). The introduction of IER brought in measures to reduce electoral fraud, which utilised data matching to confirm the legitimacy of applications to register to vote. The process is designed so that an elector's personal identifiers submitted in an application are transmitted securely for data matching against existing records to confirm their identity. The process does not aggregate or bring citizens' data together in a new way, but safeguards the privacy of the data by only providing an indicator to the local authority whether the elector's details have been matched or not, which will then prompt further action as necessary. IER and the adopted approach to handling data was consulted upon widely, extensively debated in Parliament, and is supported by all main political parties and non-party bodies concerned with the running of elections, as well as the Information Commissioner.

17. Though there are clear benefits to data sharing, many citizens have concerns about the privacy of the data they provide to public bodies, such as how their data is used and who has access to it. To address this there are a number of laws, which set out how data should be handled. The most important of these is the Data Protection Act 1998 (DPA), which enshrined in law a number of key principles about the handling and use of personal data. It is important that any steps to use data better to improve public service delivery work are taken within the framework of the DPA (and other laws) and do not weaken the protections that the framework puts in place.

18. Consultation carried out by the Law Commission during their work on the scoping report on data sharing between public bodies indicated that there is a wide variety of public attitudes to data sharing and varying levels of public trust. Any measures to increase data sharing would need to strike the appropriate balance between privacy and public benefit. Furthermore, any proposals would need to inspire and maintain citizen trust by defining clear accountability, ensuring that data sharing processes are transparent, and that controls are in place in any proposed data sharing regime to ensure the protection of privacy rights.

19. From the public sector perspective there are a number of challenges to sharing data between public bodies. The first of these is the complex legal landscape. The Law Commission scoping report, Data Sharing between Public Bodies[3], describes how the law surrounding data sharing is complex, with powers to share data scattered across a very large number of statutes. They may be set out expressly or implied. The report identified that there are problems in practice and that there are in practice differing interpretations of the law governing the sharing

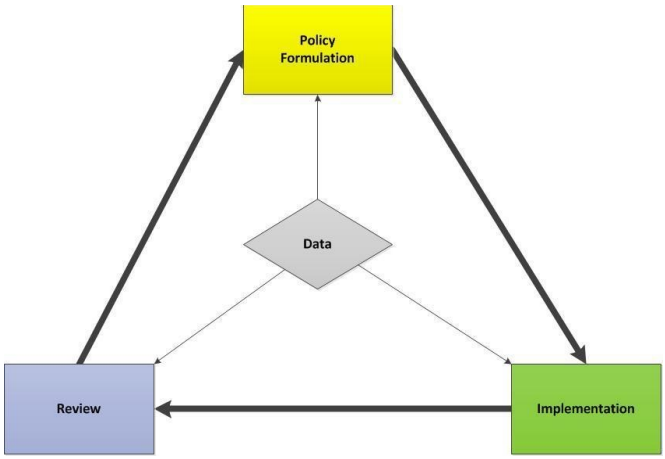
[3] http://lawcommission.justice.gov.uk/areas/data-sharing.htm

of data.

20. Understanding the complex legislative landscape around data sharing can be difficult. There have been instances where public bodies have decided to introduce specific statutory powers where data sharing is required rather than understand what existing legislation permits. The process of bringing in such explicit powers can cause significant delays and additional cost. Such delays to the sharing of data can prevent early intervention or action for those most at risk. The addition of specific powers also risks increasing confusion by creating even more specific statutory powers.

21. After some initial background work on data sharing issues, an open policy making process was launched in March 2014. Three specific problem areas were identified to be explored through the open policy-making process, with the objective of developing recommendations for policy and legislative solutions where appropriate. The findings set out in this paper are the conclusions of those individuals who participated in the OPM process and do not represent the view of HM Government. The three areas were:

    - Research and Statistics - making it easier for accredited researchers to access linked administrative data sets in accredited secure data access facilities, and speeding up the access the Office for National Statistics (ONS) has to data for statistical information;
    - Fraud, Error and Debt - looking to build on and improve the way we use identifiable data across boundaries to prevent and reduce instances of fraud and error, and help citizens to better manage debt with government in a more holistic way; and
    - Tailored Public Services – maximising the benefit of data already held by public bodies to deliver public services tailored to individual needs.



22. The three areas identified represent different stages of the policy cycle and opportunities where better data could improve the services offered for public benefit. Research and statistics provides the evidence base, which informs policy formulation and operational decisions. Tailored public services concerns how policy can be better implemented so that the front-line has the information required to ensure the right services are offered to those in need. Fraud, error and debt is a good indicator of the challenges of implementing and reviewing the success of policy to reduce waste and help citizens to better manage debt with government in a more holistic way.

Part 2 – Joint Policy Options

1 – Research and Statistics

A) Linking of de-identified data for research for the public good

The situation

23. The aim of the proposal is to ensure that public bodies (apart from health services bodies and adult social care bodies that are specifically defined) are able, if they so wish, to engage, for the purposes of research, in the process of linking two or more datasets from two or more data controllers in a way that is de-identified for the intermediaries and end-users (and is therefore privacy enhancing) using a Trusted Third Party (TTP) Sharing system which has been accredited under the legislation. A Trusted Third Party system will ensure that identifying data and payload data are always kept separate when handled by any party to the share other than the original sources. A glossary is attached at Annex A. A diagram of how the TTP sharing could work is set out below.

24. The December 2012 report from the Administrative Data Taskforce, *"The UK Administrative Data Research Network: Improving Access for Research and*

Policy"[4] recommended that "primary legislation should be sought to provide a generic legal gateway for research and statistical purposes that enables efficient access to, and linkage between, administrative data held by different government departments, agencies and other statutory bodies."

Evidence for and against change

25. Examples from government, academia and the third sector of the successes of accessing linked administrative data sets are contained in Annex C, together with the difficulties experienced in gaining access to linked data sets. This suggests that easier access to data would assist research, within government and outside, including for example: improving the family justice system; examining the drivers of productivity growth; energy saving and consumption; offending and employment; the creation of indices of deprivation; design of a local council tax scheme for vulnerable groups; housing and planning policy; and enabling the National Council for Voluntary Organisations to inform policy around fundraising. The policy is aimed at research that is in the public interest, of which the foregoing are merely examples.

26. The Economic and Social Research Council (ESRC) and ONS commissioned research from Ipsos Mori published in 2014. The findings suggest that the public would be broadly happy with administrative data linking for research projects provided (i) those projects have social value, broadly defined (ii) data is de-identified, (iii) data is kept secure, and (iv) businesses are not able to access the data for profit.

27. Provided the safeguards of running an effective prospective accreditation scheme are properly implemented by the accrediting authority, no evidence against this change has been presented to the Open Policy Making Group. Concerns that de-identification "does not work" are sometimes expressed in the media, but this is not borne out in the Report of the Administrative Data Taskforce and other recent reports. The possibility of de-identification through the use of privacy enhancing techniques is also acknowledged by the Information Commissioner's Office.

Options identified and appraised

28. The following options were identified and appraised (full details are set out at Annex D):

    a. a broad generic power: a general power for any and all public authorities to disclose identified data to each other for research and statistics; at the

[4] http://www.esrc.ac.uk/collaboration/collaborative-research/adt/

Open Policy Making Plenary meeting on 22 October 2014, members of Civil Society, present in person and by proxy, made it clear that they felt that this option would be a step too far.

b. a power for a single data controller to use a safe haven to process or disclose their own data for research or statistical analysis;
c. do nothing; and
d. a power for public authorities (except health services bodies and adult social care bodies that are specifically defined) to link de-identified data for research using accredited bodies and TTP sharing (recommended approach - see below).

Recommended approach

29. A power to ensure that all public bodies (except health services bodies and adult social care bodies that are specifically defined) in respect of all personal data relating to service users) are able, if they so wish, to engage, for the purposes of research, in the process of linking two or more datasets from two or more data controllers using only accredited bodies and a particular method of sharing called a Trusted Third Party Sharing system. The data linked in the secure access facility and made available to the researcher under controlled conditions is de-identified.

30. Data linked under the power could be used for statistics produced by a variety of Departments, as illustrated in Annex C. Our recommendation is that this power would be subject to certain exclusions:

    a. Specifically defined Bodies delivering health services and adult social care should be excluded because clinicians, patients and members of the public have all expressed serious misgivings about sharing confidential health information for secondary purposes. Further to a consultation in 2014, the Department of Health has decided not to establish Accredited Safe Havens – secure environments where identifiable information can be processed for secondary purposes and is, instead, moving faster to an ‘end state’ where data handling and linking to support health and care commissioning is done within the secure and lawful environment of the Health and Social Care Information Centre (HSCIC);
    b. processing of personal data for any purpose other than research, e.g. processing for operational purposes;
    c. the sharing of data from a single data holder to a researcher; and
    d. processing that does not involve the use of de-identified accredited third party data matching.

31. The proposals outlined in this section of the policy paper would ideally apply throughout the United Kingdom. Cabinet Office is currently engaging with officials from devolved administrations in Wales, Scotland and Northern Ireland to determine whether there is interest in applying the policies at all, identically, or with particular differences in their areas.

Scope

32. The Cabinet Office examined the existing position and surveyed a variety of public bodies. This revealed that many could already engage in Trusted Third Party Shares, however even amongst those that could they could not all do so in all circumstances.

33. Consequently the recommendation is for legislation that is restricted to two particular areas:

    a. The first is to provide any public body that needs it with the necessary power to engage in trusted third party data shares linking de-identified data with one or more other sources for the purposes of research.

    b. Secondly given that the previous area described above is wide in both the scope of the bodies it would apply to, and in the scope of the material covered, it is appropriate that the proposed legislation would also need to include explicit safeguard provisions. Therefore it has been proposed that, additionally the vires provision is made subject to a condition that it may only be used when all the bodies and individuals involved in a data share (other than the data sources) are accredited bodies. The legislation would therefore also need further provision allowing for the appointment of an accreditation body to have oversight over a process of accreditation for those wishing to partake in such shares. The accreditation body would accredit all the Trusted Third Parties including the indexers, the researchers, the secure access facilities and the research itself. While minimum accreditation requirements could be set out in the legislation, the accreditation body would themselves develop and publish additional detailed standards and requirements to attain and maintain this accreditation.

34. The detail of the rest of the administrative process as regards Trusted Third Party Sharing would need to be agreed between the parties on a case-by-case basis and be governed by the overarching law such as the DPA and share-specific agreements. Additionally any requirements of the legislation (such as accreditation) would only apply to Trusted Third Party Sharing that was relying upon the vires provision in the legislation (by at least one of the data sources).

Any public body who already had sufficient vires to undertake such sharing would be able to continue to do so outside of the new provisions, provided none of the sources of data involved needed to rely on the new power; they would not be bound by any of the requirements of the proposed legislation (such as necessity of using only accredited bodies), though they would of course remain bound by any other applicable laws, notably the DPA.

35. Based on the policy development in this area, previous reports on this subject and development of the proposals with internal and external stakeholders, definitions for key terms as regards the particular circumstances of the proposed legislative provisions have been developed. These are contained in Annex A. These are subject to change and will be further refined through further consultation and work with Parliamentary Counsel if the policy proposal is taken forward. The purpose of this glossary is to illustrate effectively the circumstances intended to be covered by the proposed legislative provisions but the legislation that results may define terms in a different way, e.g. so as to ensure consistency and clarity in the law more widely.

Accreditation body

36. The identity of the accreditation body could be specified in the legislation or there could be a power in the legislation to specify the identity, for example by secondary legislation. The characteristics of an accreditation body would be: independence, expertise in statistical research and analysis, and reporting directly to Parliament. The UK Statistics Authority is an example of the type of organisation that could be the accreditation body.

Possible safeguards

37. The detail of the accreditation scheme will be determined in due course as this policy develops. Minimum requirements might be:

a) Accredited Secure Data Access Facility (ASDAF): cannot be one of the data sources in a particular data share (though a data source can be an ASDAF for another person's data in a different data share), must be fit and proper, and ensure that researchers are only ever given access to de-identified data, and that only aggregate (i.e. not individual level records) data can leave the control of the ASDAF or be published or disclosed by researchers.

b) Accredited Indexer: could not be one of the data sources, must be fit and proper and prevent data from being removed or disclosed from the

Indexer contrary to the terms of the share, the requirements of the accreditation, or any legal or contractual prohibition.

c) Accredited TTP Researcher: must be a fit and proper person, conducting approved research in the public interest. It is understood that the Administrative Data Research Centres are not currently planning to consider private sector research requests for data. As a matter of policy we do not intend to exclude the possibility of private bodies or persons becoming accredited researchers.

d) Accredited TTP research: research in the public interest, which could in particular include (i) increasing knowledge about social and economic matters, and (ii) assisting in the development and evaluation of public policy. The outcome of the research would have to be published. Note that the Administrative Data Research Network (ADRN) is establishing an Approvals Panel (Including lay membership) which will approve research if it fulfils all of the following conditions:

a) necessary (i.e. the information does not exist elsewhere);
b) feasible;
c) of scientific merit (i.e. be worth asking);
d) has assessed and mitigated privacy issues;
e) has gone through a formal ethics review;
f) benefits the public; and
g) will be published.

38. The accreditation body would publish the names of the approved researchers, and the purpose for which the research has been approved, and would require a plain English summary of the outcome of the research. Declined requests for accreditation could also be published to support transparency and build citizen trust.

B) Identified data for research and statistics

The situation

39. Nothing stays the same. Society and the economy are constantly changing, bringing fresh challenges to Government. The policy responses to these challenges must be based on evidence that helps policy makers to understand underlying causes – to ensure that interventions are appropriate, properly targeted and make the best use of public funds. Evidence is also needed to monitor the effectiveness of Government policies, and to hold policy makers to account.

40. Independent, high quality statistics have a vital role to play in a democracy and, to provide these, it is important that statistical producers have access to as wide a range of data as possible. This includes access to data collected by public authorities as part of their routine business. These administrative data, particularly when they are linked and matched with data from several sources, can provide a rich and flexible source of evidence about how society and the economy are changing.

41. Currently, when a new policy issue arises, it is not easy for statistical producers in Government to gain access to information from administrative data sets that are held by other departments. Data sharing raises complex legal and policy issues which are open to different interpretations. This leads to an understandably cautious approach on the part of data owners. It can take months or years to reach agreement about whether a data source is relevant, and whether it can be shared. In the meantime, policy makers sometimes find themselves forced to make decisions without a comprehensive evidence base.

The legal framework: the Authority and ONS

42. The Statistics and Registration Service Act 2007 (SRSA) established the Statistics Board and set out its powers. The Board is now known as the UK Statistics Authority ("the Authority"). The Authority reports directly to Parliament and the devolved legislatures, rather than through Ministers. The Authority has oversight of ONS. ONS is the Authority's executive office; it is the UK's National Statistical Institute and the UK's largest producer of official statistics. For the rest of this document, ONS is referred to when describing the executive arm of the Authority.

43. The remit of the Authority, and therefore ONS, is limited by the SRSA (ss8-28) primarily to:

a. producing official statistics;

b. promoting and assisting in statistical research; and

c. providing statistical services.

44. The SRSA defines official statistics (s6(1), a definition which is broader than those statistics produced by ONS. The Act also requires the Authority to produce a Code of Practice for Statistics. The Board must keep confidential personal information held by it (s39) and its unlawful disclosure is a criminal offence.

45. Information disclosed to the Authority under the powers of access to information discussed in this document would in practice be provided to ONS.

The Current Legal Framework for Sharing Identified Data with ONS

46. At present some departments are able to use existing powers to disclose information to ONS. For example the Home Office shares Border Agency data with ONS for the purpose of migration statistics.

47. The SRSA contains other powers to allow certain identified data to be provided to ONS.

48. Sections 42,43 and 44 allow certain limited types of identified data to be supplied to the Authority in respect of births and deaths and NHS registration in England and Wales.

49. Under s45 HMRC may disclose some information to the Authority, but not personal information, other than for import or export statistics. This is one aspect of the SRSA that the Cabinet Office, with ONS and HMRC support, is seeking to amend.

50. Where no other data sharing gateway or power exists, or where the disclosure of information is expressly prohibited, s47 allows the Minister for the Cabinet Office to make regulations, called Information Sharing Orders (ISOs), to authorise a public authority to disclose information to the Authority to enable the Authority to carry out one or more of its functions under the SRSA (but not to provide statistical services).

51. The Cabinet Office, with the support of ONS, is seeking to amend these provisions because the s47 power is subject to significant limitations:

a. ISOs may only remove a barrier contained in a rule of law or an Act passed before the SRSA, and therefore not one that came into being after 26 July 2007. As a result the ONS is unable to use an ISO to access information where the prohibition on disclosure came into force after that date. ONS has found that, in practice, teams working on Bills since then have been reluctant to add a data sharing clause with the same effect as s.47 to their Bills, even when the departments support the principle. This is because of the potential to disrupt the passage of the Bill over what is considered to be a secondary issue.

b. Although ISOs can be used to create gateways where none already exist, ONS has found that the time taken to obtain agreement from the relevant departments can be considerable. Much of this is due to the need to resolve the uncertainties about whether a new gateway is necessary. Only then can work begin on establishing whether there is a sound justification for the data share. Experience has shown that this can be a lengthy process taking many months.

c. Reflecting the general caution around data sharing, and specific concerns about being able to obtain Parliamentary approval, the practice has apparently become established for each ISO to specify the purpose, the variables and data items required, and how the data can be used. ONS has found that excessively cautious regulations create three major problems:

    i. they lack the flexibility needed to operate effectively: they prevent reuse of data for other, previously unforeseen statistical purposes without a further ISO;

    ii. cautious drafting has sometimes made implementation of an ISO difficult because it cannot reflect the complexity of the operational systems on which the data are held. For example, the Disclosure of Social Security and Revenue Regulations were unable to be used in practice: the wording of the Regulation placed limitations on the data that could be provided. This made it impossible for DWP to provide the data because of the way their systems were designed; and

    iii. this approach is impractical where large-scale datasets with many attributes are involved (this can run to several thousands). Without new legislation proposed in this document, ONS assesses that it is likely that this cautious approach will continue.

d. The need to seek approval from Parliament before ONS accesses data makes it very hard for ONS to carry out the feasibility work required to develop the case needed to secure Parliamentary approval.

e. Once agreement has been reached that data sharing is justified and a new gateway is needed, the ISO is drawn up. Before it can come into effect, it must be approved by Parliament through the affirmative resolution procedure. Once before Parliament draft orders cannot be amended, if one point causes concern, the entire order falls. The Parliamentary procedures around affirmative resolutions had, according to ONS, been found to add at least an additional six months to the overall time taken before data can be shared.

f. ISOs may not under s47(2) be used for ONS to acquire information to provide statistical services. These are defined in s22. This restriction is thought to have originated in a desire to ensure fair competition in securing survey work. However, it also prevents ONS from acquiring information for the purposes of statistical services in relation to public authorities.

Evidence for change

52. There are several benefits from providing easier, quicker, but safe access to identified data so that it can be used for statistics. These are:

a. Efficiency – maximising the benefits of administrative data held by Government by collecting data once and using it many times, and reducing the burden on businesses and other respondents;

b. Improving policy making decisions based on research and statistics by strengthening the evidence base for policies – enabling new statistics and fresh insights on social and economic change to be developed in a timely way so that they can contribute to public debate and inform policy makers early on; and

c. Improving the quality of statistics - access to a wider range of identified data will make statistics more relevant, more timely and more reliable, and can reduce some of the uncertainties around small but significant changes emerging from survey results.

53. This section sets out some examples where easier access to identified administrative data can help to improve the evidence base and accountability of policy and decision making.

New Policy questions: new statistical outputs

54. Some policy changes emerge over a period of time in response to broad, gradual societal change. Others arise very quickly, in response to sudden changes or specific events. Statistics must keep pace with these changes and provide evidence about the effectiveness of particular policy interventions. Increasingly, policy makers need to understand the impact of their interventions on different sectors of the economy or society. In these cases, new outputs are essential to inform wider debate about societal or economic changes.

Pensions

55. Currently, ONS does not have sufficient information about employer and employee contributions to pension schemes. Matching employee data from the Pay As You Earn (PAYE) system to employer records on the business register held by ONS would enable analysis by size and type of business, as well as estimates of the value of employee contributions to the National Employment Savings Trust (NEST).

Understanding the UK Economy at a Time of Change

56. National Accounts (GDP) are the primary indicator of the nation's wealth and of the health of the UK economy. Access to individual-level PAYE data could enable ONS to provide:

    i. better quality estimates of the contributions of different industries to GDP and the income of people working in different industries;

    ii. better data on the state of the economy in different parts of the country which would give policy makers more accurate information to develop local economic policies; and

    iii. more rigorous quality assurance, based on individual data, improving the estimates for users and the transparency of production from source data to final estimate.

57. There would be additional benefits for ONS responding more quickly and effectively to new challenges, quickly developing new estimates to reflect the changing economy.

Reduced respondent burden and reduction in survey costs

58. ONS collects information through surveys, which people and businesses have already provided to Government for administrative purposes. Getting access to these data would allow ONS to reduce the burden placed on respondents to produce the vital macro-economic, population and social statistics that the UK needs to support policy making and inform debate.

Reducing the Burden on Business

59. Access to Corporation Tax and Income Tax data would contribute to on-going work to minimise respondent burden, reduce costs for businesses and for ONS. At present ONS business surveys require around 1.25 million responses from over 250,000 businesses each year. Responding to these surveys is estimated to take over one million hours and cost businesses over £22 million per year. Some of this information is already submitted to HMRC in Corporation Tax, Income Tax Self-Assessment and PAYE returns.

60. Giving ONS access to this information would enable the size and scope of surveys (e.g. Annual Business Survey and Monthly Wages and Salaries Survey) to be reduced, resulting in savings to businesses in the order of £4 million per year. The additional coverage and scope of administrative data would facilitate the production of better quality statistics and improve efficiency by reducing the need for business to provide ONS with information which they have already supplied to the Government for administrative purposes.

Improving Population Statistics

61. Good population statistics underpin resource allocation at the national and local level and are fundamental for policy formulation, decision-making, research and outcome monitoring. In addition, such statistics inform decisions on the allocation of regional aid and enable the UK to fulfil international obligations. A key source of information has been the 10-yearly census. Over the past three years the Office for National Statistics (the Beyond 2011 Programme) has been researching new approaches to counting the population. While this work has demonstrated the potential for the future production of population estimates, more work is needed. Following a careful assessment of the statistical research, the findings of an independent review of methods conducted by Professor Chris Skinner, public attitudes research and the responses to the public consultation, the National Statistician recommended that the Authority should make the best use of all sources, combining data from an online census in 2021 with administrative data and surveys. The increased use of administrative data will not only enhance statistics from the 2021 Census and improve statistics between censuses but offer a springboard to the greater use of administrative data and surveys in the

future. Such an approach has the potential to improve the accuracy, frequency and efficiency of existing statistics and the potential to provide new statistics for topics such as household income which could not be collected in a census because of concerns about data quality. The Government has welcomed the National Statistician's recommendation.

Delivering efficiency and improving statistical quality

62. Improving statistical quality has a direct impact on the quality of the evidence provided to policy makers, enabling decisions to be based on more timely, relevant and comprehensive information.

Improvements to the Business Register

63. The Inter-Departmental Business Register (IDBR) holds information on UK businesses and is widely used by the Government to provide information on the structure of the economy, for labour market statistics and to conduct surveys. The IDBR uses company registration data to help match VAT/PAYE records to identify which businesses to include in a business survey sample frame. However, company registrations do not indicate trading status or economic activity (many company registrations are made for non-trading purposes). The companies' registration system holds over 3m live companies, whereas the IDBR only contains around 1.4m of these. Of the remainder, it is possible that a proportion is actively trading but are under VAT/PAYE thresholds, and as a result are not included.

64. If ONS had access to Corporation Tax records this would enable identification of businesses that are actively trading, and would improve the coverage of small businesses. This could allow ONS to capture changes in the economy more quickly and provide more responsive analysis.

Labour Market Statistics

65. There are three key labour market series produced by ONS – workforce jobs; unemployment and employment measured through the Labour Force Survey (LFS); and the claimant count. Statistics on the number of jobs in the UK are collated from a quarterly business survey. Access to PAYE real time information from HMRC would potentially allow monthly rather than quarterly publication of these statistics and increase the accuracy of the figures by drawing on data from a much greater number of businesses. Policy makers looking at the labour market would have access to improved and more regular estimates of the number of jobs. Being able to consider these together with claimant count statistics and the sample survey-based estimates of employment from the LFS would allow policy

makers to identify trends in the labour market with greater confidence. Access to these administrative data would also enable an improved understanding of the characteristics of all three data series, which could facilitate quality improvements to the statistics in the future.

Linking data for other public authorities

66. As part of ONS's collaboration with the Administrative Data Research Centre (ADRC) for England, it will link data from public authorities, including data held by ONS, and provide disclosure controlled outputs to approved government researchers in safe-settings. This function is covered by existing provisions in the SRSA (s23 “promoting and assisting statistical research”).

67. ONS will use these existing powers but have assessed it would be able to fulfil this function more effectively with a speedier alternative to the Parliamentary process for accessing information from public authorities.

Options considered

68. The proposal is to create powers that would enable identified data held by public authorities to be shared for the Authority’s functions (which are primarily statistical). The potential benefits that could result from streamlining access to identified data from administrative sources are set out above. In considering the options, it is important to: prevent the misuse of data; ensure that the data acquired can be used only for statistical purposes; and, ensure that no identifiable information about individuals is unlawfully disclosed.

69. The following options were identified and appraised (full details are set out at Annex E):

- Option 1 - No change to the existing arrangements;
- Option 1a – Temporary permissive power for the Authority;
- Option 2 - Remove restriction in SRSA s45 (5) on personal HMRC information;
- Option 3 - Permissive power for the Authority; and
- Option 4 - Broad power for all public authorities to share identified data with each other for research and statistics. At the Open Policy Making Plenary meeting on 22 October 2014, members of Civil Society, present in person and by proxy, made it clear that they felt that Option 4 would be a step too far.

Existing Safeguards That Would Continue

Legal safeguards specific to The Authority[5]

70. Disclosure of information held by the Authority is restricted by law: s.39 SRSA contains a criminal penalty for unlawful disclosure. In addition, the Authority and ONS are subject to the Data Protection Act, the law of confidence, and the Human Rights Act 1998. Breaches of the Data Protection Act can result in enforcement action, including fines, by the Information Commissioner. In addition, data disclosed to ONS are subject to specific terms and conditions agreed between the data owner and ONS. Similarly, unlawful disclosure of information covered by the Social Security Administration Act or the Commissioners for Revenue and Customs Act 2005 would constitute a criminal offence under these acts. Researchers approved under s.39 (4)(i) of the SRSA would also be subject to contractual constraints and penalties in accordance with arrangements set out in data access agreements made by the Authority; ONS employees are subject to disciplinary procedures under their contract of employment.

Governance

71. ONS is independent of ministers and, as the executive office of the Authority, operates at arm's length from government. Governance of the Authority is set out elsewhere in this document. The SRSA sets the Authority the objective of promoting and safeguarding the production and publication of official statistics which serve the public good. The Authority and ONS are unable to exercise any functions outside the SRSA.

Policy safeguards

72. The Authority and ONS must comply with the Government's Security Policy Framework. This provides the basis for assessing and managing risks and protecting key information assets. As a result ONS must uphold standards for information assurance, data security and risk management including those promulgated by CESG (the National Technical Authority for Information Assurance) and the International Organisation for Standardisation (IOS). Such standards cover: data transfer, systems, procurement, reporting and training.

---

[5] In general, Authority would remain subject to the Data Protection Act, the law of confidence, and the Human Rights Act 1998, in respect of the information it received. A serious breach of the data protection principles also attracts liability for monetary penalties levied by the Information Commissioner's Office. Data disclosed to ONS is subject to specific terms and conditions agreed between the data owner and ONS. Researchers approved under s39(4)(i) of the SRSA will also be subject to contractual constraints and penalties under data access agreements under which the Authority discloses information to them; ONS employees are also subject disciplinary procedures under their contract of employment.

73. Where relevant, other processes/procedures may include the completion of the appropriate type of privacy impact assessment and/or an independent review of security arrangements (e.g. those undertaken for the 2001 and 2011 Censuses). In addition, ONS would need to comply with specific departmental requirements/ conditions including clearance or approval from bodies such as the Data Access Ethics Committee in DWP and the Data Management Advisory Panel in Department for Education (DfE); including the ability to fully inspect the facilities, and audit data handling processes and procedures.

74. All staff must sign the ONS Confidentiality Declaration to confirm that they understand their obligations to keep information safe and secure and the penalties associated with any infringement of ONS statutory and other related obligations.

75. The ONS Information Charter[6] explains how ONS carries out its responsibilities for handling personal information (in addition there is a 'Respondent Charter for Business Surveys' and a 'Respondent Charter for Households and Individual Surveys). Easier access to administrative data, and being able to match and link information for statistical purposes will help ONS to meet specific pledges in their Information Charter only (e.g. to ask for only what is needed).

76. Ethical requirements are contained in the Code of Practice for Official Statistics, especially those covering Integrity, Confidentiality and the Protocol for Use of administrative sources for statistical purposes.

77. Any direct collection of data for testing or evaluation purposes complies with the principles set out in the Code of Practice for Official Statistics. The Code contains principles and practices that are intended to ensure that: the range of official statistics meets the needs of users; that the statistics are produced, managed and disseminated to high standards; and that the statistics are well explained.

Security

78. Government has set out, in its HMG Security Policy Framework[7], the standards, best practice guidelines and approaches that are required to protect UK Government assets. This sets the minimum obligations for the Authority. Personal accountability for data is ensured by the requirement, under this Framework, to appoint and train, for each data asset, an Information Asset Owner

---

[6] http://www.ons.gov.uk/ons/about-ons/business-transparency/information-charter/index.html

[7] Version 11 – October 2013
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/299556/HMG_Security_Policy_Framework_v11.0_doc.pdf

(IAO), who is responsible for it. ONS has produced a handbook[8] for the use of IAO. Data are transferred in accordance with the Security Policy Framework. When required CESG-approved encrypted media are used with encryption passwords and/or tokens controlled by either ONS Security Managers or the Security Managers in the owning Department.

79. ONS has published examples of their approach to safeguarding data[9]. In accordance with Government requirements; when working with data, ONS imposes the following controls:

- Physical security - access to ONS buildings is controlled and monitored;
- Personnel security- all personnel are subject to security checks to the level required for their role; and
- Procedural security – all data acquisition, import and export processes are subject to strict procedural controls, in many cases incorporating separation of duties.

80. ONS recognises the security risks of handling identifiable data and has taken some specific measures when linking and matching across disparate datasets. For example, data anonymisation processes were developed for the Beyond 2011 Programme. ONS has implemented a range of processes to ensure that appropriate levels of anonymity and privacy are maintained where appropriate.

81. Data export and publication are carried out in accordance with the SRSA and Code of Practice for Official Statistics whereby no personal information about an individual is disclosed in any statistical output. All outputs from ONS research are subject to Statistical Disclosure Control (SDC), that is methods designed to protect individuals, households and businesses (and their attributes) from identification in any published tables or other statistical outputs.

Procedures

82. The Authority has set out the process that is currently undertaken when negotiating and agreeing the acquisition of data under the current SRSA regulations (see Annex F). The purpose of these procedures is to determine that:

- the information is of sufficient quality;
- the information is actually required;

[8] The Information Asset Handbook (ONS v1.8 May 2014)

[9] http://www.ons.gov.uk/ons/about-ons/who-ons-are/programmes-and-projects/beyond-2011/reports-and-publications/beyond-2011-safeguarding-data-for-research-our-policy--m10-.pdf

- the proposed data share complies with existing legislation including the DPA and the Human Rights Act; and
- privacy risks and issues have been addressed appropriately;
- security requirements and standards have been met and account has been taken of its impact on the business and statistical outputs of ONS.

83. The terms used in Annex F are explained in a document entitled “Stepping Stones”, which provides guidance for members of the Government Statistical Service to use when considering data sharing applications for statistical or analytical purposes[10].

Accreditation process

84. The Authority is currently permitted to disclose personal information that it holds to an approved researcher for statistical research. It publishes the criteria applied to secure accreditation as an approved researcher as well as the measures taken to assess the suitability of individual research projects[11].

New oversight safeguards options as alternatives to the Parliamentary Process

85. Under SRSA s.47, ISOs are approved by affirmative resolution in both Houses of Parliament. Affirmative resolution fulfils two functions:

- legal authority for the data share; and
- independent scrutiny of the proposal to ensure that the business case is robust and the conclusions justified.

86. ONS has found that the affirmative resolution process adds approximately six months to the time it takes to get a data share, therefore new options are proposed as alternatives to the Parliamentary process. Any alternative approach to scrutiny and decision making must have the same, or greater, rigour; ONS does not wish to limit scrutiny in any way. However, in order to achieve increased efficiency and flexibility to inform timely policy decisions ONS is keen to ensure that legal approval for any proposed data share can be made quickly and easily.

The current approach: Information Sharing Orders and Affirmative Resolution in Parliament

[10] http://www.ons.gov.uk/ons/guide-method/best-practice/gss-best-practice/stepping-stones-to-data-sharing-for-statistical-purposes/index.html

[11] http://www.ons.gov.uk/ons/about-ons/business-transparency/freedom-of-information/what-can-i-request/approved-researcher-accreditation.html

87. Many steps precede the Parliamentary process to ensure that a proposal is appropriate and lawful. There are extensive discussions between ONS and the data owner to identify and substantiate the requirements for access to the data. ONS conducts a full legal review, establishes the statistical and business case and carries out a privacy impact assessment. Governance arrangements vary between data owners: in some cases the proposed data share must be reviewed by a departmental ethics committee or equivalent, in others it must be reviewed at Board level. These steps provide internal scrutiny and ensure that, from the perspective of the data owner, the share is appropriate, legal, proportionate and ethical. This work is essential and should continue to be part of any data sharing process.

88. Once Officials, lawyers and Ministers agree that an ISO is appropriate, and Ministers whose consent is required are content and satisfied that the conditions at s.47(9) are met (including the public interest test), the ISO is reviewed by the Secondary Legislation Scrutiny Committee, which considers the proposal to identify whether it:

- raises issues around legal, political or public policy; or
- is inappropriate because circumstances have changed since the relevant primary legislation was passed; or
- inappropriately implements European Union (EU) legislation; or
- imperfectly achieves its policy objectives.

89. Once the regulations have been scrutinised and endorsed they are laid for consideration by relevant committees in the House of Commons and the House of Lords. A short debate follows, informed by any issues raised by the Scrutiny Committee. There is no scope to amend the Order; it stands or falls as laid.

90. Hansard shows the depth and nature of the debates for the five ISOs that have been laid. The number of attendees at the debates has ranged from two to fifteen; the length of debates is usually 15-30 minutes; the longest debate lasted 40 minutes (this was the first ISO), the shortest debate lasted one minute. The debates rarely consider the details of the data share, but instead discuss wider issues related to it (for example, the importance of the Census, or data security). Assuming the Order is approved by both Houses, it is signed by the Minister for the Cabinet Office and other relevant Ministers and becomes law.

91. There have been strong representations from some elements of Civil Society that the Parliamentary process should be sacrosanct.

<u>Possible alternatives to Affirmative Resolution</u>

92. A key principle that has underpinned the consideration of alternatives to Parliamentary scrutiny is the need to ensure that decisions are made at an appropriate level, by a person or body which can be held to account.

93. The place for independent external scrutiny of data sharing proposals has also been considered. Independent scrutiny provides support to those making decisions about complex or unfamiliar issues, and assures the public that the proposal has been considered from an external perspective. It should be transparent, with decisions and advice made public. It should be rigorous, giving detailed, expert consideration to each proposal, and provide assurance that the proposal:

- is in the public interest;
- is lawful;
- supports a valid statistical purpose; and,
- appropriately reflects practical issues such as compliance with government security policies and standards.

94. Three options have been identified (details are provided in Annex G):

- Option 1: ISOs approved by Affirmative Resolution (Do Nothing)
- Option 2: Decision by Minister
- Option 3: A new power to replace s.47 with involvement of an Independent Ethics and/or Approvals Body in the decision making process. There are four further variants of this option.

95. No consensus has been reached as to a preferred option.

96. Any decision would need to involve the Devolved Administrations.

C) HMRC Strand – Sharing general, aggregated and de-identified data for public benefit

The situation

97. HMRC is a statutory body, created by the Commissioners for Revenue and Customs Act 2005. This imposes a duty of confidentiality on HMRC officials, which applies to all information that HMRC holds in connection with its functions. A criminal sanction protects against the unlawful disclosure of information that identifies a person or through which their identity can be deduced (called "identifying information" for the purpose of this section of the paper). HMRC may share information only in limited circumstances set out in legislation, in particular:

- For the purposes of HMRC's functions; or
- With the consent of each subject of the information; or
- Through specific legislative gateways

98. Once it has a valid legal basis enabling disclosure, HMRC must ensure compliance with the Data Protection Act and Human Rights Act, alongside practical elements - resource implications etc.

99. HMRC holds sensitive information and it accepts that it is right for there to be a strong focus on any information sharing proposals. However HMRC holds a spectrum of information ranging from non-identifying through to identifying information that is extremely sensitive in nature. It is therefore arguable that the current protections offer more protection to, for example, non-identifying information, than is needed and that a more tailored approach could be taken, accounting for sensitivity and risk, with appropriate safeguards to ensure that confidentiality is not compromised.

100. HMRC identified three specific information types that it considered to be at the lower end of this sensitivity spectrum and in 2013 consulted on specific proposals for the wider sharing of these information types, including a proposal to share general, aggregate and de-identified data for purposes wider than HMRC's functions to generate public benefits.

General and Aggregate information

101. General information is information that is not, nor ever has been, identifying information, for example, information on policies and processes.

102. Aggregate information is grouped information, summarising the characteristics of a set of data. This is potentially more disclosive than general information, but still generally low risk within the spectrum of information types that HMRC holds because it is not disclosed on an individual-level basis. Where HMRC is currently able to disclose this type of information, it does so using safeguards that are appropriate to the data type. This includes employing strict security and information management processes, and robust statistical disclosure policies. Permissive powers mean that disclosure is not mandatory and the criminal sanction protects against unlawful disclosure of identifying information (which could occur if, for example, the aggregation was at too granular a level).

103. If HMRC could share this information more widely by way of a broad gateway enabling disclosure of aggregated data for the purpose of delivering public benefits, HMRC could contribute to the more efficient and effective delivery of services and benefits beyond HMRC's functions, for the benefit of UKplc.

De-identified data

104. De-identified data cannot directly identify an individual, and so does not amount to personal data under the first limb of the definition of Personal Data under the DPA. This data could nonetheless potentially amount to personal data under the second limb of the definition if the individual to which it relates could be identified from the combination of that data with other data held or likely to be held by the data controller.

105. HMRC currently provide access, under strictly controlled conditions, to this type of data for research purposes. However, those research projects must be able to demonstrate a benefit to HMRC's functions, limiting the potential to deliver research for public benefits beyond HMRC's functions.

106. Recognising the greater risk of a customer's identity being deduced than in the case of aggregate data, the following safeguards are currently in place and will remain unchanged under the proposal:

- A secure and controlled environment provided by HMRC's Datalab[12], which has been operating successfully for over 3 years;

[12] http://www.hmrc.gov.uk/datalab/about.htm

- Only projects with a valid research purpose and from trusted organisations are allowed. HMRC expects publication of the findings from the research;
- Users undergo a rigorous accreditation process and need to sign an agreement with HMRC on the use of the information;
- Datasets are de-identified, and statistical disclosure controls are carried out on any research outputs before they leave the Datalab;
- Researchers are subject to the same confidentiality provisions as HMRC staff, including the criminal sanction; and
- The environment and processes are consistent with the recommendations in the 2012 Administrative Data Taskforce Report for the safe sharing of data for research and statistical purposes.

107. The proposal seeks to provide a legal gateway which will allow research to be undertaken for wider public benefit and not just, as currently, for HMRC's functions.

Evidence for and against change

108. Left as the status quo, HMRC will, as now, be approached with requests to disclose information, which will be considered on a case-by-case basis. If a valid legal basis is available that could allow disclosure, HMRC will need to consider any data sharing options or proposals, i.e. the need to ensure compliance with the Data Protection Act and Human Rights Act, alongside practical elements - resource implications etc. However if a valid legal basis is not available, this has to be provided for before disclosure can be made. A legislative vehicle needs to be found and the process of creating a statutory gateway can typically take up to two years.

109. The proposal would enable a broad gateway to be implemented by reference to information type (i.e. general and aggregated data, de-identified individual level data), where this would lead to 'public benefit'. Having this gateway in place would allow HMRC to contribute to a wider range of government initiatives than it currently can and for purposes beyond HMRC's own functions. In particular, a broader gateway could improve the evidence base for policy-making and promote knowledge sharing between research organisations and the public sector.

110. The absence of a legal gateway can frustrate wider policy formulation and development and addressing these data needs by the usual way of a new legal gateway on a case-by-case basis is time-consuming and resource-intensive. HMRC accepts that identifying information (especially financial information) is

sensitive and should be subject to rigorous and on-going scrutiny and critical assessment. However if less sensitive data types (with safeguards as appropriate) were available under a broad gateway, not only will HMRC be contributing more effectively to wider initiatives with a view of delivering public benefits on a broader scale, but government departments could be encouraged to seek less sensitive data by way of this existing gateway (if implemented) rather than the default of seeking a new gateway for potentially identifying information.

111. Listed below are some examples of approaches for HMRC's information that have either had to be turned down or have had to be substantially modified:

- An approach was made to HMRC to supply anonymised data to help the Chief Medical Officer for Wales to carry out research into the factors underlying excess winter mortality. Considerable work was undertaken to identify whether and how the information could be disclosed. Obtaining customers' consent to disclose anonymised data was not practical, there was no link to HMRC's functions and legislating a specific gateway would have been too time consuming and would, in any case, have been too late to inform the research. The conclusion was therefore reached that it would not be possible for HMRC to supply the requested information.
- Department for Business, Innovation and Skills (BIS) applied to use the Datalab to produce tables of profits turnover, counts of total and loss making companies by turnover size and industry sectors using Corporation Tax. The aim of their project was to:
    - investigate the relationship between company profitability and deposit holdings for the non-financial corporate sector by company size and industry sector; and
    - quantify the issue of companies only able to pay interest on debts with no ability to invest and grow their business.

  This was rejected by The Datalab Committee because assessing companies' productivity did not fall within HMRC's functions.
- The London School of Economics (LSE) were hoping to match HMRC data to the Annual Business Inquiry from the ONS to inform a paper on the determinants of outsourcing of business services, a sector that plays a vital role in the U.K. economy (Globalisation, Managerial Complexity, and Service Outsourcing). This was rejected as it did not

fall within HMRC's functions.

- The Bank of England was unable to conduct research to investigate the relationship between the prices charged by individual firms and total sales, their costs and other characteristics. They wanted to do this by analysing income (and productivity) profile of self-employed individuals and matching data from Consumer Price Index to HMRC PAYE data (to get information on wages) and VAT returns (to get sales, inputs and value added) within the Datalab. This approach was unsuccessful as the project was beyond HMRC's functions.

112. In addition, responses to the public consultation in Summer 2013 were supportive of this proposal, as long as the safeguards were sufficient to protect confidentiality (particularly in case of de-identified data). As noted above, HMRC already makes this type of information available, with strict safeguards, for research that links to HMRC's functions and has done so successfully for over three years. However HMRC understands the concerns raised and, as previously noted, will explore other proposed safeguards as part of the consultation process.

Options identified and appraised

113. The proposals for wider sharing of general, aggregate and anonymised data set out in this paper and the earlier consultation document were informed by HMRC's experience of disclosing these data types, where it is currently legally able to do so. HMRC was able to offer up safeguards that are currently applied successfully, while seeking views on these.

114. It is proposed that the purpose of the legal gateway should be framed in terms of delivering public benefit. Public benefit would be judged by an approvals committee within HMRC, which might include external representation. The argument that such a body should be within HMRC rather than an external body, is based on the fact that it is de-identified data that is being provided. This is similar to the approach adopted by UK Statistics Authority in disclosing information in its Virtual Microdata Laboratory to accredited researchers, as empowered under s39(5) of the SRSA. The proposed approach to framing the purpose of the gateway is informed by the experience of earlier unsuccessful requests for HMRC data which had to be turned down because, in order to provide the data, a specific link was required to HMRC's functions. An alternative approach would be to specify a purpose 'beyond HMRC's functions', but this would result in a far broader gateway than a provision tied to 'public benefit'; in addition, 'public benefit' is considered more in line with the public's expectation of what Government departments' policy and initiatives should be framed around.

However HMRC is aware that there needs to be clarity on what exactly is meant by public benefit and welcomes the open policy making process as a means by which this can be explored. For example there is a formulation of “public good” in the Statistics and Registration Services Act (s7(2)) ’public benefit includes in particular (a) informing the public about social and economic matters, and (b) assisting in the development and evaluation of public policy’.

Proposed Method for Delivering the Recommended Approach

115. HMRC proposes that the legislation should provide the necessary structural framework for a permissive (not mandatory) legal gateway for each of the information types (i.e. for general and aggregate information and for de-identified individual level information) together with the purpose, alongside the main safeguard of a criminal sanction protecting against unlawful disclosure (of information that identifies a person or through which their identity could be deduced). However HMRC considers that in order for the gateway to have sufficient flexibility for the future, that there will need to be elements that are maintained outside of legislation, for example through a policy statement and/or a code of practice which could be provided for in statute. HMRC would be looking to develop this aspect, picking up on similar elements being developed by the new Administrative Data Research Network.

116. By way of illustration, a policy statement could be used to set out the statistical disclosure tests that HMRC applies to aggregate information, with the aim of ensuring that it will not be possible to deduce information about identifiable individual persons from aggregate information; the criteria used to assess public benefit; governance of Datalab research requests[13]; accreditation/vetting processes; publication of the identities of those approved as accredited researchers; publication of the subject matter of research that has been approved; and the requirement for a plain English summary of the outcome of the research to be published.

117. This is a different proposal to the Trusted Third Party strand of the data sharing proposals. This is because in these proposals there is a statutory bar within the Commissioners for Revenue and Customs Act 2005 (CRCA) which needs to be amended in order for HMRC to make data available to others in HMRC’s own

[13] For example HMRC is open to considering the establishment of an HMRC-led advisory committee with independent representation to consider applications to access HMRC data for the purpose of public benefit.

safe setting, whereas the Trusted Third Party strand is designed for two or more sources of data, the de-identified data being available in a third place, the ASDAF.

118. HMRC currently asks other government departments to cover HMRC's costs in providing data to them and would expect that other government departments would account for this element, when determining the costs and benefits of their policies.

2 - Fraud, Error and Debt

The situation

119. Fraud and Error, as a cost to the whole UK economy, stands at **approximately £73bn with approximately £20.3bn being attributable to the public sector**. [14] Whilst this is an indicative figure it may not be completely accurate as there are unquantifiable considerations, such as the activity of the shadow economy, which will always require a degree of educated assumption. The work carried out by the Fraud, Error and Debt team within the Cabinet Office estimate that this cost could be within the range of **£38bn - £67bn**. This represents a range of **2.62% - 5.03% of GDP**. This has been based on the data from the Annual Fraud Indicator and comparator data from European countries and the US as well as current thinking on issues such as the shadow economy.

120. Government estimations of fraud and error include a £22bn known fraud loss and a loss of approximately £14.5bn in relation to error. These were based on the Annual Fraud Indicator (mentioned above) and are therefore subject to the same issues as set out above. They are also complicated by factors such as the definition of error not being uniform, and therefore have been rightly questioned during the open policy making process. Our proposals seek to gather evidence that would give a greater understanding of the full costs of Fraud and Error.

Evidence for and against change

121. Wider use of data sharing could improve the prevention, detection and investigation of **Fraud and Error** by:

a. aiding better targeting and risk-profiling of potentially fraudulent individuals;
b. saving taxpayer's money by streamlining processes; and
c. increasing the ability for Government to act more quickly on fraud and error by simplifying the legislative landscape.

122. There are clear calls to increase the effectiveness and/or the efficiency of current data sharing from across the public sector and some private sector organisations. These are based on a reported lack of flexibility (the difficulty in adapting to changing circumstances in a timely fashion given legislative processes), the complexity of navigating the current legislative landscape and the time taken to create new data sharing relationships. A working example of the

[14] The most recent Annual Fraud Indicator (published March 2012 and found at: https://www.gov.uk/government/publications/annual-fraud-indicator) document sets the cost of Fraud and Error to the UK Economy as a whole as £73bn and provides a useful breakdown of this by sector.

issues faced by the Charities Commission when they set up a successful data-matching pilot is provided in Annex H.

123. Simplification of current processes, either through legislation or, where sufficient legal authority already exists, through increasing public sector skills, knowledge and general capability in data sharing matters, would be beneficial to government. A case study of the arrangements in place between Department for Work and Pensions and HM Revenue and Customs, which has simplified their data sharing through the use of a broader gateway, is provided in Annex I.

124. For **Fraud and Error**, participants in the open policy making process identified a number of challenges and clarifications needed to fully understand the evidence base and therefore provide a robust basis from which to assess whether further intervention is required.

a. What **barriers** frustrate data sharing for Fraud and Error, what are the **incentives** that drive data sharing?
b. What existing gateways aren't being used? What is the level of public official awareness of what can and can't be shared?
c. What is the **public attitude** to data sharing to combat Fraud and Error?
d. What are the **costs and benefits** of improved data sharing to combat Fraud and Error, can they be fully quantified (costs and benefits as defined in their broadest sense: privacy, financial etc)?
e. What is the comparative value of **different approaches** (data analysis as opposed to validating data or validation and analysis in combination; case by case validation and analysis as opposed to bulk data validation where it is necessary and proportionate)?
f. How do we **strike the right balance** between efficiency and effectiveness on one hand, and privacy on the other?

<u>Barriers</u>

125. There are a number of barriers that the group felt may frustrate the sharing of data, including the complex legal landscape and a risk averse culture. A further specific key barrier relating to Fraud and Error is resource.

126. Sharing data requires resource. Organisations that hold a lot of data are often responsible for major functions of government (the administration of the benefits system for example) and have to make hard choices about how best to deploy their resources. At a more personal level, if data sharing is not somebody's 'day job' it is unlikely to be a priority for the person to respond to requests to do so.

127. It is clear that without a full understanding of the drivers, barriers and incentives for data sharing, then a proposal may be put in place that may not then be fully effective. At the same time without testing out some new approaches, it is unlikely that a full understanding of how the incentives operate will be reached.

Costs, Benefits and the Comparative Value of Different Approaches

128. Many of the proposed benefits of data sharing in this area are derived from assumptions relating to isolated case studies that have proved successful. For a robust decision these benefits need to be clearly articulated and underpinned with evidence that can be scaled up to the point where it is effective without losing sight of the costs of intervention. Testing out potential interventions would improve our understanding of what the benefits would be and how easily they could be scaled up.

129. The costs of improved data sharing also needs to seek to take into account, as far as possible, the individual cost of intervention on top of the financial and resource implications of different approaches. Whilst some of the costs may be clearer the social impact may not be fully understood without testing out some of the proposals in a smaller environment.

Getting the Balance Right: Privacy v Effectiveness and Efficiency

130. The OPM process agreed that to ensure a solution is effective, it would need to take into account the financial costs and benefits as well as minimise intrusion on individual privacy, particularly of individuals who would not be of interest in relation to fraud. To achieve this balance, evidence would need to be gathered about how effective any proposed solution would be in minimising cost in particular and ensuring that principles of necessity, proportionality and transparency are applied appropriately. OPM participants acknowledged the benefit to citizens of validating/verifying information using data already held by government rather than alternative processes which may be more intrusive and inconvenient.

131. OPM participants agreed that Privacy Impact Assessment principles would need to be embedded throughout the work to ensure that proposals would be balanced. They also supported a high level of transparency and accountability.

<u>Recommendations</u>

132. There are three Key recommendations relating to Fraud:

a. To gain a greater insight of demand for data and citizen attitudes to data use for Fraud – initially this has been recommended to be measured through surveys and deliberative studies;

b. To build up further evidence through additional case studies; and

c. To test out ways of using data through trials and pilots, to better determine the value of intervention.

133. All of this work would need to be evaluated and assessed throughout to ensure that benefits were being realised as expected and captured where new ones emerged.

134. The view of the OPM group was to prioritise recommendations (a) and (c), building feedback loops into any piloting model thereby allowing insight work to be targeted at groups directly affected. Work being taken forward elsewhere in Government would help us build the bank of case studies (recommendation (b)).

135. This concentrates effort specifically on Fraud as opposed to Error. There is good reason for this. There is very little agreement on where the line is drawn between fraud and error, making any work that specifies error separate to fraud potentially uncertain and therefore less likely to be successful. It was felt that there are non-legislative avenues to address error and it is likely that some error will be reduced through the increased data quality that work to reduce fraud will help to deliver.

Work ongoing elsewhere in Government

136. A number of pieces of work are being taken forward by Government to counter fraud that could be used in the pilots to help to increase further the evidence base to support new legislation. There are two main categories of work:

a) Work that is currently operational but that could yield further evidence or be extended to run potential pilots. This includes:

i. The National Fraud Initiative;

ii. CIFAS;

iii. Student Loans counter fraud work; and

iv. Department of Health eligibility work.

b) Work that is exploratory and non-operational, which could potentially form the basis of pilot schemes. This includes:

i. Cabinet Office – Proof of Concept work;

ii. The Counter Fraud Checking Service;

iii. HMRC/DVLA pilots;

iv. Work with the Law Enforcement Community;

v. Data sharing mapping work between Home Office, DWP, HMRC and Cabinet Office;

vi. Department for Communities and Local Government work with Local Authorities; and

137. For a fuller description of the ongoing work please see **Annex K.**

Pilot Legislation Model

138. Legislation is recommended to authorise pilot studies, which would gather evidence and better understand the value of intervention. Pilots would require appropriate governance and flexibility in its arrangements.

139. Pilots would ensure that new powers to share data are only rolled out where such intervention is justified. Work involving the exercise of existing legal powers should continue and inform the development of both the legislative powers and the pilot schemes.

140. New legislation should in the first instance only allow data sharing for the purposes of one or more pilot studies, with the powers being capable of being rolled out if the schemes are evaluated and found to have been successful.

141. New powers would be permissive and normally supplement, rather than replace, existing powers.

Process

142. It is recommended that pilot schemes are governed according to a three stage process, moving from validation to light analytics, to detailed analytics. At each stage the number of people under consideration would be reduced.

143. Organisations participating in a pilot would run the following process:

a) **Stage 1 'Validation'** – An individual wishes to transact with Government, or a government body wishes to batch process its data to check for potential fraud indicators. At this stage a pilot organisation would be able to check the information that they have been provided against information held by any other participating organisation in order to check its validity ('validation'). They would receive a binary 'yes/no'

response as to whether the information provided agrees with the information held by other participating organisations. Those that do agree do not require any further intervention. Those that are not validated in this way move to Stage 2;

b) **Stage 2 'Light Analytics'** – Results that have not been able to be validated against another organisations' information would give detail about exactly what information has not been able to be validated, revealing the information held about that field by participating organisations to the pilot organisation carrying out the transaction. This information would be restricted to only the field where information has not matched. At this stage, the pilot organisation in collaboration with the individual whose data this relates to may be able to weed out information that is erroneous. Where this can't be done the transaction would move to Stage 3[15] and

c) **Stage 3 'Detailed Analytics'** – Greater information about the individual is made available to the pilot organisation (from other participating organisations). This would allow the pilot organisation to build a picture that aids the investigation (such a process does not replace actual investigation of cases) of whether there is an issue of deliberate intent that may require further investigation (potential fraud), or whether this is a genuine error. The pilot organisation would then be able to gather information that would aid investigation into potential fraud, which would allow a case to be built or help to eliminate the suspicion of fraud. Once a suspicion of fraud exists then existing pathways are open to the pilot organisation.

Building feedback into the process

144. The OPM group considered it vital to evaluate the success of pilots. Proposed feedback would include:

a) **Measures:** At each stage output and outcome measures need to be taken that clearly determine where a case has resulted in either 'no further action' or progression to the next stage. At both stages 2 and 3 it would be important to note the reason why no further action has been taken (for example, 'error within the data identified/corrected') which would allow those assessing the pilots to understand the effectiveness

[15] It may be practical and desirable to run stages 1 and 2 simultaneously, so that where there isn't a match the return discloses the stage 2 information automatically. This certainly makes sense for both individual 'real-time' transactions and batch processing of information. This will dependent on the technical capabilities of the organisations involved. However, these have been kept separate as they are theoretically different points in the process and in some instances the technical capabilities involved will mean that it is not possible to do this without delay between the two stages.

of the intervention.[16]

b) **Feedback:** At the start of the process (Stage 1), particularly where the pilot is seeking to perform checking at point of transaction, feedback would be sought from the citizen, explaining to them what is happening, and seeking their views on how they view the intervention (did they think that this would have happened anyway, if not how comfortable are they with the process etc.)[17] Whilst consistency of approach would be important, data from this may be context-specific so it would be important for expert input in how best to collect this information so that it could be collected sensitively and objectively. Sometimes it may be the case that transactions do not go ahead as a result of feedback being sought, where this is the case this would need to be recorded and analysed as part of the overall assessment of the pilots.

Eligibility to take part in pilots

145. Organisations wishing to take part in a pilot would need to be able to prove their need to Ministers. It is envisaged that this would come in the form of a business case setting out:

a) Their data status: Are they likely to be a data supplier that holds a lot of the data that other pilots would need, or are they likely to be an organisation that needs to obtain data from another participating organisation? Every organisation is likely to be a bit of both, but the balance may be different depending on the organisation and the context.

b) The proposed pilot methodology: Where would a pilot take place and who would it involve? How would feedback be collected and collated? What would be the operational governance of the pilots and how would it feed in to the wider strategic assessment of the pilots? What are the technical capabilities and constraints?

c) The proposed costs and benefits of the pilot: What are the operational and resource costs of doing this? Have these been appropriately considered? What are the expected benefits both in terms of effectiveness and efficiency?

---

[16] Although in the majority of cases, 'error' will need further investigation to fully establish and rectify, there are likely to be a number of data errors that will be picked up through this process and the impact of this will need to be measured.

[17] Tipping potential fraudsters off prior to interview under caution would need to be minimised as far as possible, hence front-loading this process at the least intrusive stage. Such feedback gathering would have to be done in as sensitive a way as possible in order to mitigate this risk, but may have to accept that this would be an 'ideal' in some situations.

d) What alternative options have been considered? Has a non-legislative approach been considered? What are the barriers to alternative approaches?

e) Has there been any research-based work that demonstrates the concept? For example, work to test out the potential effectiveness of such a pilot (initially some of this could be demonstrated through the FED Proof of Concept and Risk Measurement work).

146. Initial indications suggest that potential participants in a pilot might include:

a. HMRC;
b. DWP;
c. DVLA;
d. Ministry of Justice;
e. Home Office;
f. Local Authorities; and
g. NHS Business Services Authority.

147. Organisations authorised to use the new powers would be set out in a schedule to the legislation, which could be amended to add or remove organisations (thereby allowing flexibility). Entry to the schedule would be contingent on demonstrated need and a willingness to abide by safeguards as set out in a separate Code of Conduct. The Code would include provisions such as submitting to the ICO for audit and assessment as required, publishing Privacy Impact Assessments to carry out the work and publishing data about the use of the powers.

148. If at any stage a participating organisation failed to abide by the Code of Conduct, or the need for the powers was not there anymore this would be reasonable grounds on which to remove that organisation from the schedule.

Governance

149. Appropriate governance needs to be in place to ensure that pilots are commenced, assessed and continued or closed as appropriate. At an operational level, this would include the usual data governance structures of Departmental Information Asset Owners and Senior Information Responsible Owners and at a Ministerial level agreement on key decisions. However, at a strategic level, a group would be needed that could steer the overall direction of travel of the pilots, take a view on proposed pilots, assess the value of the pilots and make recommendations to stop or to carry on and scale up pilots at appropriate junctures.

150. It is recommended that this Strategic Steering Group would include

representatives from Government, interested Civil Society Organisations and independent observers. It could look as follows:

a. A Policy Lead who is accountable to the Minister responsible for the overall pilots – likely to act as chairman for the group;

b. Policy leads from Government Fraud and Error teams;

c. Representatives from interested Civil Society Organisations and academia;

d. A member of the ICO with 'observer' status; and

e. Appropriate data analysts and operational subject matter experts in relation to pilots being discussed (invited for the period needed).

151. The group would meet at key points prior to and during the legislative pilots in order to look at the evidence collected (from business cases, measurements and feedback) and make recommendations. It was felt that Ministers should have regard to the advice from this group when making decisions as to whether to scale-up the pilots, but ultimately the decision to do so would rest with the Minister.

152. Transparency would need to be an essential part of this process. For example, recommendations of the Strategic Steering Group should be published.

What Would a Power to do this Look Like?

153. Not all aspects of the process and governance would need to be set out in legislation but this is subject to legal advice about how best to put the above processes, membership and governance into effect.

The Initial Power

154. The proposal is to create a 'purposive gateway' (one that is constrained by the purposes for which the data will be used). This would allow specified organisations to share information relating to an individual where this is for the purposes of prevention, detection, investigation or prosecution of Fraud, subject to a number of safeguards (listed below).

155. The purposive nature of the power alone serves as a safeguard. A further option would be to seek to limit the scope of the terms 'prevention', 'detection', and 'investigation'.

156. Potential options for this power include creating separate powers for each stage that specify the information being shared (Stage 1 and 2 the information directly relating to that provided by the citizen and at Stage 3 much broader information relating to the citizen). Or to keep the stages out of legislation itself and to make this a part of guidance or a Code of Practice.

157. The proposal is to specify the organisations involved in a list (Schedule) within the legislation. To allow flexibility it is recommended that an amendable schedule of participating organisations is created – with an Order making power that allows Ministers to add or remove organisations from this schedule. Such a power to amend would be limited to ensure that the Ministers consult with or have regard to advice and evidence when making the decision to amend.

158. Potential options considered included specifying the organisations on the face of the legislation without a power to amend by secondary legislation. This creates a much more static power that would not provide the flexibility required for testing via pilots.

159. A further set of options identified, revolve around the Order making power. This is the culmination of the advice process set out earlier (in the Governance section of this paper). There is the option to specify that such an Order would require affirmative as opposed to negative resolution in Parliament (affirmative provides higher levels of scrutiny but is more time-consuming and therefore potentially less flexible than negative). Negative resolution is recommended on the basis of the level of flexibility for quick start-up and shutdown of pilots. The option is available to specify the type of evidence that a Minister would need to have regard to when seeking to make such an Order (for example evidence of need and willingness to abide by a Code of Practice) as well as who must be consulted in the decision making process.

160. The OPM group recommended that the safeguards include a code of practice that participating organisations would need to follow in order to stay on the schedule. It was felt that the Code of Practice should contain the following key safeguards:

a. All participating organisations must submit themselves to audit by the Information Commissioner;

b. All participating organisations must publish Privacy Impact Assessments in relation to their proposed pilots;

c. All participating organisations must periodically publish the measurement data coming from the pilots – and if the power becomes fully operational to continue publishing such measurement data;

d. The process of the pilots (as set out under Stages 1, 2 and 3).

161. Options here include specifying a number, or all of these on the face of legislation as opposed to in a Code of Practice. Depending on how this is set out, this may make what is initially a set of pilots less capable of transitioning into an operational state and would therefore need further work to investigate any unintended consequences of specifying these in legislation.

162. It is recommended that it is made clear on the face of legislation that the confidentiality of information is protected.

163. Given the nature of pilot schemes, the group recommended that the legislation to allow pilots to take place should be flexible enough to allow for one or more pilots to take place simultaneously or at different times.

164. The criteria according to which Ministers would make decisions to commence or stop pilots as well as who may be consulted should be specified.

165. A minimum length of time for a pilot to run before it could be evaluated a success should ideally be specified, although the group felt that it would need to be clear about any unintended consequences of including a specific length of time before it could fully recommend such an option.

166. It is proposed that a review clause be included that ensures a review of the overall power after a specified period (probably 3 years) after commencement.

Debt

167. The recent National Audit Office report (*Managing Debt Owed to Central Government*, February 2014) reaffirmed the importance of reducing debt owed to Government as part of good financial management. The Cabinet Office and HM Treasury are working jointly to further strengthen financial processes across departments through a range of measures.

168. The current size of debt owed to the Government is approximately £22bn. Of the overall debt that is owed to Government, 88% was owed either to HMRC or DWP, 10% was owed to the Ministry of Justice and 2% owed to other departments.

169. This £22bn figure is a global amount and therefore does not represent the size of *collectible* debt (i.e. the amount of that total figure that can be collected) owed to Government. The potential sum is still likely to be significant enough to merit intervention to seek to increase the recovery of collectible debt, but this may require further investigation.

170. The Government's two key aims are to provide better support to citizens to help them manage their debt as well as to increase the amount of debt collected by the Exchequer.

Potential Benefits

171. Wider use of data sharing could increase debt recovery by:

a) ensuring the right information is available to the right department at the right time to identify debtors;

b) making effective interventions earlier to prevent debt from accruing;

c) making the process fairer, through a better understanding of the circumstances of the debtor;

d) informing strategic decision making about debt management; and

e) making debt collection more efficient, supporting work for creating a single point of access for the debtor and Government to engage. This more efficient process is also expected to be more effective, by making repayment clearer and easier for the debtor, although there are potentially issues for both public perceptions, definition of terms, and incentives that will need to be explored and resolved.

172. To understand the value of interventions and its impact on collectable debt the full benefits would need to be explored and quantified. Participants in the OPM process would welcome more clarity on:

a) collective terminology - different public authorities define debt in different ways and have different sets of terminology surrounding their activities to manage debt and there is a wider issue of what type of debt is being discussed that will determine best approaches to collecting (for example individual debt as opposed to company debt);

b) the drivers for change;

c) an understanding of what the size of *collectible* debt (as opposed to the overall debt balance) is across Government;

d) the impact that data sharing would have on raising the amount of collectible debt and helping citizens to manage their debt;

e) constraints needed to control disproportionate sharing of data; and

f) Which areas of debt to best target.

173. The scope of the debt proposals have been focused on supporting the work of the Debt Market Integrator.

Work to Support the Debt Market Integrator (DMI)

174. The DMI seeks to maximise efficiencies of Government debt collection by pooling resource into a single space.

175. It will take some debt information from a number of participating Government organisations: HMRC, DWP, Home Office, Legal Aid Agency, Student Loans Company and the DVLA and then seek to act on those separate debts on behalf of Government, being the interface between the debtor and the participating organisations.

176. The Cabinet Office has lead policy and delivery responsibilities for this, whilst data use will be tested and accredited by CESG[18].

177. Current data sharing constraints can prevent government from supporting debtors through the use of a single payment plan. This may mean that a number of debtors face being pursued for money on multiple occasions by the DMI but on behalf of the different participating organisations. For example, someone who is a debtor to three different parts of government could be approached on three separate occasions by the DMI in order to pursue the debts.

178. Without consent, the DMI operator will not always see the plans agreed for the other departments' debts, so the independent new payment plans may not be feasible.

179. A series of separate approaches can compound stress and anxiety for the debtor, as it can feel like an unmanageable level of debt is being built up. It risks the debtor taking on new payment plans that they cannot fulfil, and debtors can end up 'robbing Peter to pay Paul'. Worse still, having engaged and made the situation no better, the debtor may well disengage entirely until more formal proceedings are taken forward.

180. A single view was something that was urged by the Public Accounts Committee (PAC) in its investigation of the DMI. The PAC recognised the benefits to the debtor from a reduced number of approaches and a combined management of debt to ensure affordability, based on evidence from similar private sector approaches, which show benefits for both the business and the debtor alike.

181. Given the potential complexity of developing a single approach across all departments and bodies, the view to date had been that legislation would be

---

[18] The UK government's National Technical Authority for Information Assurance (CESG), advises organisations on how to protect their information and information systems against today's threats

necessary. The OPM group questioned the necessity for legislative measures and officials have been investigating the potential for non-legislative ways of supporting debtors through a single view.

182. While a potential non-legislative route is explored (see below), Government could carry out preparatory work for possible legislation. Such legislation would only be introduced in the event that a consent-driven mechanism is evaluated as not delivering the benefits needed.

183. At the meeting of 2 December, representatives from civil society organisations and privacy groups expressed a clear preference for a consent driven mechanism, whilst some strongly supported a legislative approach due to possible losses to HMG whilst a consent-based approach was being tested. The OPM Group conclusion was for an initial consent-driven mechanism with a fall back option of legislation was fair, so long as the assessment of the consent mechanism was objective and transparent.

184. Whilst there was overall agreement at the meeting, concerns were raised about the use of data in this way by the DMI. The existence of the DMI is not in scope of this OPM process and as a result issues raised around this and how it operates have not been captured in this paper.

Consent Driven Mechanism

185. Given data legislation, it is proposed that that the mechanism would enable debtors to opt-in to support through consenting to the DMI combining debt data and managing it as a single debt. A suggested process for how this might work is set out below:

186. **Initial contact**: on initial contact with a debtor the DMI would seek consent to see if there is any other debt held by the other participating organisations. The risks and benefits of this would be spelt out as clearly as possible. If a debtor then refuses to this the DMI would proceed with the single debt as initially envisaged. If the debtor agrees to this information being obtained the DMI would then search for other debts owed.

187. **Combining information**: The DMI, having conducted a search for other debts would seek the consent of the debtor to combine these and manage them as a single debt, allowing for the creation of a single payment plan potentially making the debt more manageable.

188. **Paying off the debt**: The single payment plan would ensure that payment back to Government occurs as per agreed hierarchies of payment, ensuring that debt

is paid off to the highest priorities and in the correct proportions from the single payment.

189. **Clearing the debt**: once the debt is cleared the consent would be deemed to have lapsed, so should the DMI need to contact that debtor about future debts, consent would need to be sought again as if it was initial contact.

Measurement and Evaluation

190. The group has agreed that in order to evaluate if the consent mechanism is effective, measures would need to be taken at each stage to understand the balance between a range of factors including:

a) **Fairness** to the debtor;
b) **Prevention** of further default;
c) **Efficiency** of the process; and
d) **Effectiveness** of the process.

191. These could be evaluated through a range of measures including:

a) **Consent** – rates of uptake and feedback;
b) **Complaints** – about the process or other; and
c) Rates of **recovery**.

192. It was also agreed that unintended consequences would need to be monitored such as potential displacement of debt (paying off debt by creating other debt which is just as unmanageable).

193. It is proposed that a Strategic Steering Group would be created, which as part of its responsibilities, would review the evidence in order to evaluate the effectiveness of the process and whether or not legislation is needed.

Legislation

194. Whilst a consent driven mechanism is the clear preference of the civil society and privacy group participants in the OPM process, commercial concerns were

raised that the potential uptake may not be as high as expected. reducing the potential benefits both to debtors and to Government; or that the balance of other benefits suggested above is not being delivered as expected. If this is the case, legislation would be required.

195. The legislative mechanism would also be subject to review and assessment (similar to that for the consent driven mechanism) in order to gauge its effectiveness.

196. In summary, the OPM group recommends that no legislation is required if a consent driven mechanism is assessed to be highly effective against clear criteria by an agreed date.

Process under legislative model – power to share data for the purposes of the DMI

197. A typical process may take the following steps:

Step 1: At the point that debt data is handed to the DMI about an individual, the DMI would be acting on behalf of the member organisations to search for debts with other participating organisations to the DMI. Where there are no other debts, no further action to join data would be taken.

Step 2: On the discovery of other debts, the DMI would check with the debtor to verify that those debts are indeed relating to that individual. If the information is erroneous, no further action would be taken to join that data.

Step 3: Where the debtor is found to owe multiple debts managed by the DMI, the DMI would inform the debtor that their debts would be joined into a single payment plan and arrange terms with the debtor for that single debt to be managed.

198. Such a power to combine data would need to be evaluated to ensure it met the benefits that it set out to do. This decision would be taken by the Minister (see below regarding governance for how advice to the Minister would be decided) based on an assessment of the power's value from the measurement of its effectiveness and efficiency as well as the feedback from citizen engagement.

199. If an assessment suggests the power is ineffective then the Minister may take the decision to cease the use of the power.

Eligibility under the legislative model

200. It is proposed that only data belonging to public authorities who are clients of the

DMI should be eligible to be joined. The following organisations are likely to participate:

a. Home Office;
b. HMRC;
c. DWP;
d. Student Loans Company;
e. Legal Aid Agency; and
f. DVLA.

201. Data would not be shared for other purposes and the DMI should not be able to pass on data except to agencies dealing with default for the pursuit of that debt.

Issues for Legislation

202. **Making clear the reason for legislating now:** Whilst the group has agreed to the plan to legislate if necessary, the group's recommendation is that **the two schemes should not run together.** The group felt this could invalidate consent.

203. There was also a note of caution that there was some risk **that the mere prospect of legislation could undermine the validity of consent**, even if the consent and (if necessary) legislative approaches happen sequentially rather than concurrently. This risk arises from the fact that, to be valid, consent must be freely given. If customers are aware that at some future point they may have no choice but for their data to be shared, it might be argued that "consent" is not truly freely given. This was deemed an acceptable risk that required monitoring and review over the coming period.

204. The **transition** from consent to legislative authority for data sharing where it doesn't already exist is not fully clear. Individuals may have volunteered more information than would be available via legislation. They may have ongoing debt management plans. Initial thinking on this is that those plans set up through consent would continue as per the consent so only new plans created would be through the legislative mechanism, were it to come into force.

205. **Different organisations are sending different categories of debt to the DMI:** some organisations are asking the DMI to handle all their debt, some are only handing over difficult to recover debt. As such, there may be a question around specifying the type of data capable of being shared by departments/ organisations. Several options are being discussed and the most practicable will be included:

a. Specifying the data on the **face of the legislation**, whilst on the face of

it looks the most certain route, could actually lead to a number of ambiguities and complications. The different types of debt handled means that you could not simply specify a single type of data that could be shared and therefore may end up with a different set of clauses for each organisation. At the outset this may be acceptable (with 6 organisations), but as the DMI may expand in the future, new amending legislation would be needed with each new organisation added (either done through primary legislation or creating a very wide order making power to amend the primary legislation).

b. Specifying the data in an **amendable schedule** to the legislation: this suffers from less of an issue than that of option a but the complexity would remain.

c. Specifying the data shared in a **code of practice** that all organisations must have regard to with a penalty for not doing so being to not be able to use the new powers. This seems to be the most straightforward and was the one most agreed to by the group.

d. **Remaining silent** about the data. This, whilst the most flexible, was not really discussed by the group, and seemed least palatable when it was discussed.

e. **Setting a maximum ceiling** of data that can be shared in the legislation. This allows for more flexibility within constraints that could allow for the right balance of constraint and the ability to take on new organisations without having to amend legislation each time (other than the schedule of organisations).

Governance

206. The group felt that governance of the consent-based scheme should involve a Strategic Steering Group. There would be checkpoints built into appropriate parts of the process to evaluate evidence and recommend continuation of the consent-based mechanism or, later, the power.

207. The strategic level governance could be constituted from a range of groups including:

a. A policy lead responsible for data sharing;

b. Policy lead from the team responsible for the DMI;

c. Debt leads from participating organisations;

d. Operational lead/s from the DMI and participating organisations;

e. Representatives from interested Civil Society Organisations; and

f. A member of the ICO (to be present as an observer).

208. Transparency would be an essential part of this process. Recommendations from the Strategic Steering Group should be published.

3 — Tailored Public Services

The situation

209. For Britain to lead the world in transformative public service design and delivery in the context of increasingly reduced finances, public agencies will need to work ever closer together to identify new ways to support citizens. Legal restrictions around data sharing between public agencies are increasingly frequently cited as a critical barrier to the design and delivery of public services in new ways. The current legal context is highly complex, and multiple barriers prevent data sharing across and within public agencies. These hinder the ability of the government to protect the most vulnerable and to achieve improved outcomes for citizens. The results of barriers to data sharing include:

- public agencies are not able to share data to identify accurately which citizens are eligible for a particular service or benefit and therefore to ensure that the right people receive it;

- overlap, contradiction and gaps between services provided to an individual; citizens receive disjointed and fragmented services from a range of agencies as their needs change during their lifetime;

- reactive service delivery which means citizens often receive support too late; and

- public agencies cannot free up time for citizens by exchanging information internally so citizens are required to repeat their information multiple times and spend significant energy and time meeting bureaucratic requirements.

210. Effective policy is only as good as its delivery. This proposed power intends to enable Government policy to be effectively delivered by ensuring that those individuals most in need of a particular intervention receive it: ‘making the right offer to the right person at the right time’.

211. To address these issues and to ensure that public services are delivered in a manner which is ‘person focused’ the following policy has been developed through a process of iteration and testing with multiple stakeholder groups.

Recommendation

212. ‘A permissive power for *defined public agencies* to share data with *defined public agencies* for the purposes of improving the delivery or targeting of public services in specified areas of social policy[19], resulting in an offer of help to an individual. This power is intended to operate in accordance with a number of principles:

- The intent of the power is to help individuals by making sure that they are offered the right intervention at the right time;
- The power is not designed to be punitive or detrimental to the individuals in question (although this does not mean that if benefit fraud is uncovered through use of the power it would not be addressed; but this could not be the *purpose* of a data share under the power)[20];
- Data matched but not used for the purpose described in the business case will be disposed of according to relevant information governance processes and not used for any other purpose; and
  The business case (for the specific data share) includes - *details of the intervention and how it will enable the achievement of the objective*.

<u>Examples of objectives that could be included</u>

- Improving education and employment outcomes for young people who are considered ‘Not in Education, Employment, or Training’ (NEET) or whose activity is not known
- Improving health, education and employment outcomes for individuals with multiple public service dependencies;
- Reducing the number of people sleeping on the street for more than one night;
- Improving employment outcomes for ex-offenders;
- Supporting gang members to safely exit gang culture;
- Supporting the fuel poor to improve their health outcomes;
- Prevent homelessness amongst those leaving hospital to improve health outcomes;
- Prevent homelessness amongst those leaving prison to reduce reoffending rates;
- Identify individual family member problems, link the data to understand the multiplicity and complexity of these problems across the whole family in order

---

[19] “Social Policy is focused on those aspects of the economy, society and polity that are necessary to human existence and the means by which they can be provided. These basic human needs include: food and shelter, a sustainable and safe environment, the promotion of health and treatment of the sick, the care and support of those unable to live a fully independent life; and the education and training of individuals to a level that enables them fully to participate in their society.” (http://www.lse.ac.uk/socialPolicy/Home.aspx)

[20] Under the Data Protection Act, personal data can be used in ways that sometimes may cause a detriment to the individuals concerned without necessarily being unfair (not being entitled to a benefit or a priority recipient of a service). What is important is whether the detriment was unjustified. Relevant link: https://ico.org.uk/for_organisations/data_protection/the_guide/conditions_for_processing).

to deliver services that reduce offending and improve health, education, employment and life outcomes;
- Improve employment outcomes for people experiencing entrenched worklessness; and
- Reduce reoffending rates amongst ex-offenders.

Examples of objectives that would not be included under the power

213. In considering how to safeguard a power from being too broad participants in the OPM process agreed that specifying some acceptable example policy objectives would be helpful. Similarly the OPM group felt it equally, if not more, important to specify example policy objectives for which the proposed power would not apply. These latter examples thereby provide a barrier to constrain the extent of such a power.

- Improving levels of safety in a neighbourhood (this doesn't focus on the benefit to the individual);
- Improving safety in an area through identifying those with criminal intent (this is punitive);
- Identifying individuals operating in the grey economy (this is punitive);
- Identify welfare claimants erroneously receiving welfare benefits (this is punitive);
- Help people into work (too broad); and
- Prevent people going to prison (too broad).

214. The term 'public bodies' in the proposed power is not a pool of agencies which can share data, but rather the ability for specified public agencies to be able to share data with other specified public agencies/ specified departments in a local authority, in a defined direction, determined by policy need. Current public bodies recommended for inclusion are listed below. This incorporates defined types of public agency as well as individual public bodies.

- Central government departments and their executive agencies;
- Local authorities;
- Local health care providers and commissioners. Use of this power by local health providers, or by other parts of the public sector seeking access to health data, would be conditional on involvement of an appropriate expert panel, such as arrangements similar to S251 of the NHS Act 2006 and subject to oversight by the Independent Information Governance Oversight Panel; and

- Devolved administrations (should they wish to participate).

215. While it is recognised that there is increasing fragmentation of public service delivery across the public, private and third sector, this policy focuses only on public bodies delivering public services. This will result in significant improvement in the delivery of services to citizens while protecting citizen data.

Policy rationale

216. The power would meet the objective of facilitating data sharing where it would directly benefit service recipients, by enabling agencies to better tailor services, but also protects privacy by restricting the agencies and the purposes involved in any particular share quite tightly. It is sufficiently future-proofed to meet data sharing needs of public policy delivery in the future, while ensuring that the privacy of individuals remains paramount.

217. A permissive power to share data for the purposes of delivering or targeting of public services, resulting in an offer of help to an individual fits well with the DPA and would support organisations to meet the fair processing and transparency requirements of the DPA. The ICO's statutory Data Sharing Code of Practice emphasises the importance of having a clear purpose or objective (or set of objectives) for sharing data. Being clear about what the sharing is meant to achieve can also help organisations decide what data they need to share, with whom and whether the sharing is justified and proportionate. Data sharing arrangements can then be designed with this purpose in mind.

218. This power is intended to be used in situations where:

- The objective could not be met without data sharing.
- It is *not realistic and practicable* to use consent to achieve the intended outcome or use of consent would not meet the criteria of free and informed decision.
- Sharing and analysis of anonymised data would *not achieve the intended* outcome.

For more detail on the process see figure 1.

219. The recommendation is that the objectives should be capable of being amended through secondary legislation to reflect future changes in social need and in social policy while still ensuring that individuals benefit from use of their data.

Other options identified and appraised

220. A very broad power that would enable public agencies to share data when it is in “the public interest.” However, in the group’s view, this would not adequately balance needs of privacy and the protection of individual rights with the public interest and as a result there was no consensus on this approach.

221. Specific gateways that provide the legal ability for public agencies to share information on a case-by-case basis. However, the three key disadvantages to this are:

- The time, cost and political process required to legislate means that government will always lag a few years behind meeting the data sharing need identified to improve service to citizens and in some cases the need will not be met at all;
- A case-by-case approach leaves the development of safeguards up to individual cases; this limits the ability of government to set up a robust framework of safeguards that will be applied consistently to data shares, as would happen with the recommended option; and
- It would not meet the key objective of future proofing the policy.

222. No legal change to the current situation and a focus on cultural change. This would not address the legal barriers to sharing data to tailor public services better to individuals and therefore not solve the problems identified. This programme of work will supplement the cultural change work in local places lead by the Centre of Excellence for Information Sharing.

Safeguards

223. Even where a permissive power is conferred, a final decision by an agency to share data would be subject to the DPA Article 8 of the European Convention on Human Rights (ECHR), any additional protocols/safeguards imposed across the OPM’s data sharing proposals, existing statutory codes of practice and the department’s own guidelines.

224. The interaction between the new power and existing statutory gateways and frameworks are to be considered further.

225. A new power would contain three key ‘layers’ of safeguards: the primary power, which limits the use of the power by the wording; the requirement to go through an affirmative process in Parliament to add an objective to secondary legislation; and a detailed process of what needs to be in place to implement the power, which includes key safeguards such as an accountability in decision making and publication of the Privacy Impact Assessment (see figure 1).

Method of delivery

The process for sharing TPS Data using the flexible gateway

226. Figure 1 demonstrates the process for deciding to use the new power, and how this relates to the other work streams in the broader data sharing work.

227. Department A seeks data held by Department B. The proposed data share meets the criteria of the TPS power and therefore there is a legal gateway. Department A sends a business case to department B. It is the prerogative of Department B to agree, or not, to Department A’s proposal.

228. Key elements for inclusion in the business case are:

- The entire route of the proposed data share, e.g. from Department B to Department A, further internal disclosure/matching within Department A, and any onward disclosure to Local Authority C or Agency D;
- How it meets the legal gateway criteria i.e. how the proposed data share would benefit the end user;
- Costs and how these would be divided; and
- Fit with Government and Departmental priorities, i.e. *departments/ authorities involved should avoid taking action which would be contrary to core business/functions*.

229. The decision making processes within departments/agencies are up to the department /agency, but the decision as to whether to agree to a data sharing process using the TPS power should be taken at a level of seniority on or above the agreed minimum level. The recommendation is that a Senior Responsible Officer (SRO) for data sharing be appointed at Board level. Departments/public agencies currently have their own processes for managing information and making decisions about data sharing.

230. Department B, as the data controller, would also make any decision to share data conditional on certain requirements being met. It is expected that these would include universal/internal standards for data and information storage, disposal, governance and assurance. It is recommended that data shares follow

up-to-date industry-recognised standards and best practice. All parties would in any event be required to comply with the seventh data protection principle in the DPA that ‘appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data’.

231. Once agreement has been reached in principle, parties will proceed towards drafting the Information Sharing Agreement. Key supporting documents will include Impact Assessments, the most relevant here being the Privacy Impact Assessment (PIA).

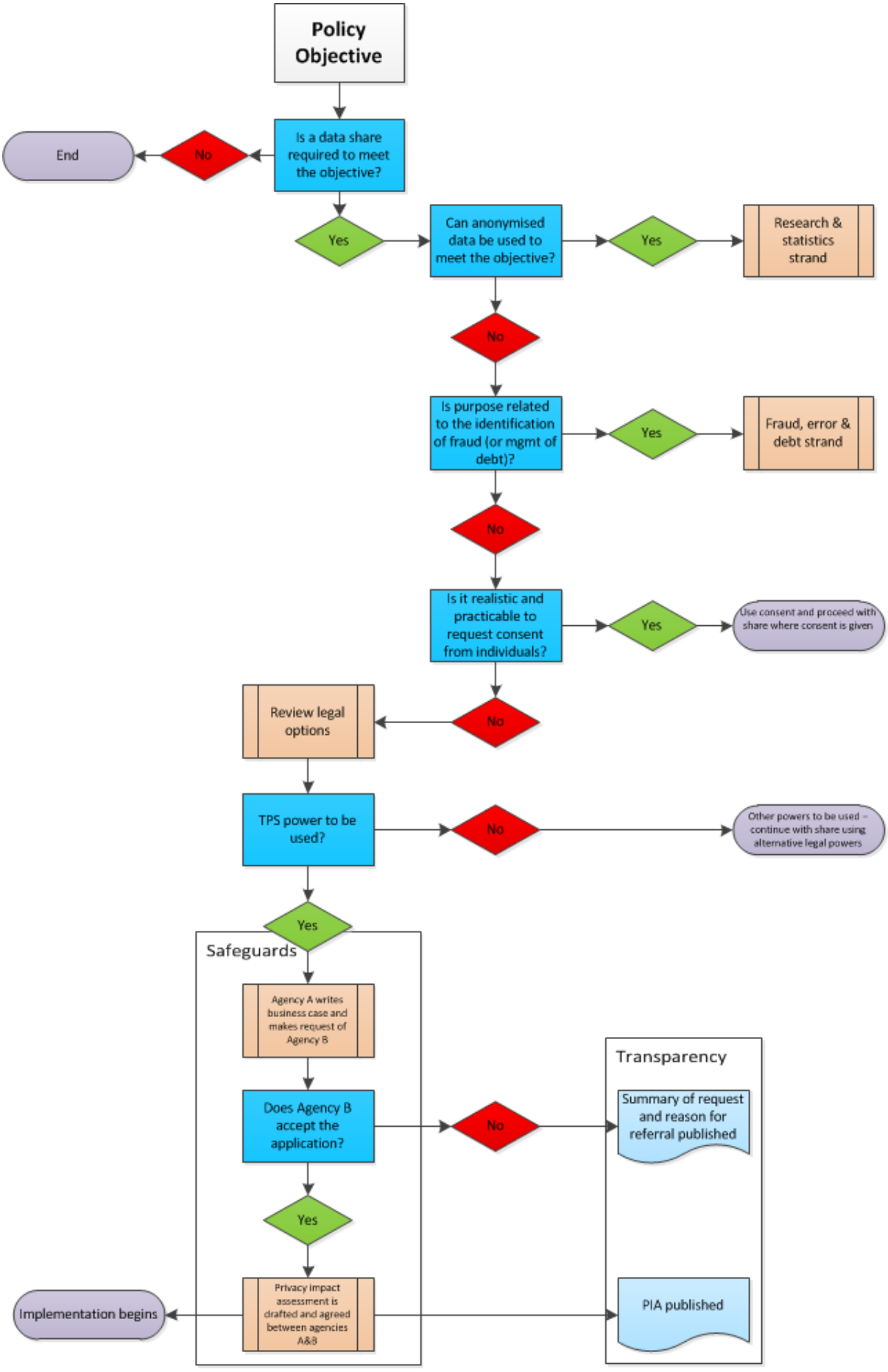

Policy Objective
Is a data share required to meet the objective?
No
End
Yes
Can anonymised data be used to meet the objective?
Yes
Research & statistics strand
No
Is purpose related to the identification of fraud (or mgmt of debt)?
Yes
Fraud, error & debt strand
No
Is it realistic and practicable to request consent from individuals?
Yes
Use consent and proceed with share where consent is given
No
Review legal options
TPS power to be used?
No
Other powers to be used – continue with share using alternative legal powers
Yes
Safeguards
Agency A writes business case and makes request of Agency B
Does Agency B accept the application?
No
Transparency
Summary of request and reason for referral published
Yes
Privacy impact assessment is drafted and agreed between agencies A&B
Implementation begins
PIA published

Figure 1 – Decision process for proposed new power

Thematic issues

Criminal Offences and other penalties

232. Criminal offence for unlawful disclosure of personal information (similar to CRCA 2005, DWP legislation such as Social Security Administration Act 1992 s123, and SRSA 2007) would apply to all bodies when using the power. DPA section 55 would also apply to any people knowingly or recklessly obtaining or disclosing personal data, as would s.55A DPA (the IC's power to serve a monetary penalty notice on a data controller for a serious contravention of the data protection principles.

Oversight of the data sharing process

233. Currently Parliamentary committees consider data sharing issues on a 'subject based' basis as they arise. This oversight can range from detailed inquiries into data handling such as the Health Committee's inquiries into the handling of NHS patient data to more specific recommendations on data sharing by Select Committees as part of wider reports into specific programmes, for example the Work and Pension Select Committee's report on Universal Credit and the Energy and Climate Change Committee's report on fuel poverty. The Public Accounts Committee also makes recommendations on data sharing on cross government initiatives for example in its report into programmes to help families facing multiple challenges.

Transparency

234. It is proposed that the following be published at least two weeks ahead of the final decision being made on implementation, and any comments received would be considered in taking that decision:

- A list of data shares agreed under the power, and a summary of their purpose; and
- The PIA produced for each share – see the ICO website (https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/) for further information on PIAs.

Future Proofing

235. To make the power flexible and future proofed, the policy objectives and the public bodies would be amendable through secondary legislation going forward.

236. Data sharing is intrinsically linked to changes in technological capability. For this reason it is recommended that a regular review of the impact of new technology on data sharing safeguards be instigated, and where necessary safeguards added/amended in order to ensure that the policy continues to deliver the intended objective in light of technological advances.

Quality of data

237. The DPA already places a statutory duty on all data controllers to take adequate steps to ensure that data is accurate and where necessary up-to-date.

Onward disclosure /Use of data beyond the purpose for which it was shared

238. The power would only permit onward disclosure with the permission of the originating department; and only where a lawful power existed for that onward disclosure and it complied fully with all applicable DPA and HRA requirements.

Additional protections of personal data:

239. The following key measures are recommended to further protect personal data:

- Relevant trials/pilots should be used to ensure the data sharing or linking meets identified objective. This is a chance to test whether the criteria for the share can be met, as well as to explore if the policy objective can be achieved through the data match. If the pilot does not demonstrate the expected benefit then an alternative data share will not be rolled out;
- Where practicable and realistic consent will be used and individuals will be asked permission to share their personal data with other agencies (e.g. older people and people with disabilities);
- Personal data will only be used where fully anonymised data would not meet the objective; and
- Minimisation of data shared. In every case departments will ensure that the personal data shared is limited to those data necessary to achieve the objectives.

Part 3 – Conclusions

240. The recommendations set out in this paper are a result of an open and productive dialogue between officials from a number of government departments and other public bodies, civil society and privacy organisations. Where the rationale for change has not been sufficiently robust, such as with initial proposals relating to fraud, strong challenge by civil society groups have shaped recommendations that aim to better understand the problem and the value of intervention. Where the case has been compelling, such as with tailored public services, it has been some of the active participants from civil society organisations from the OPM group that have pushed to go further in defining how broad a power should be to provide longevity. These are strong indicators that the process has been successful and that all those participating have listened and shaped the work.

241. These recommendations are the culmination of a significant amount of engagement and commitment and energy from a large number of people from within and outside government. The sensitivities around the issue of data sharing require a sensible dialogue. The opportunities to transform public services afforded by technology and more effective use of the data already held by public bodies are great. Understanding privacy concerns and factoring them earlier into the policy development process may help realise some of those opportunities. However, wider consultation is required so that the views of more people and organisations can be heard to ensure proposals strike the right balance between preserving the privacy of citizens' data and enabling public sector cross-referencing of information before proposals are implemented. Further engagement is also required with the Devolved Administrations.