

Consultation Response Data Sharing Open Rights Group

Name (optional): Javier Ruiz

Position (optional): Policy Director

Organisation name: Open Rights Group

Address: 12 Tileyard Road, London, N7 9AH

Email: javier@openrightsgroup.org

Telephone (optional): 07877911412

Would you like us to treat your response as confidential?*

If you answer yes, we will not include your details in any list of people or organisations that responded to the consultation.

Yes No

Is this a personal response or an official response on behalf of your organisation?

Personal response

Official response

If you ticked "Official response", please respond accordingly:

Type of responding organisation*

Business

Charity

Data sharing consultation ORG

- Local authority
- Central government
- Wider public sector (e.g. health bodies, schools and emergency services)
- University or other higher education institution
- Other representative or interest group (please answer the question below)

Non profit campaign group, not registered charity _____

Type of representative group or interest group

- Union
- Employer or business representative group
- Subject association or learned society
- Equality organisation or group
- School, college or teacher representative group
- Other (please state below)

Digital rights campaigners _____

Nation*

- England
- Wales
- Northern Ireland
- Scotland
- Other EU country: _____
- Non-EU country: _____

How did you find out about this consultation?

- Gov.uk website
- Internet search
- Other

Data sharing consultation ORG

____Participating in open policy making_____

May we contact you for further information?

(x) Yes () No

Introduction

Open Rights Group is the UK's leading digital campaigning organisation, working to protect the rights to privacy and free speech online. With 3,200 active supporters, we are a grassroots organisation with local groups across the UK. We believe people have the right to control their technology, and oppose the use of technology to control people.

Digital technology has transformed the way we live and opened up limitless new ways to communicate, connect, share and learn across the world. But for all the benefits, technological developments have created new threats to our human rights. We raise awareness of these threats and challenge them through public campaigns, legal actions, policy interventions and technical projects.

ORG has engaged extensively in the open policy making process for more than two years, since we were first approached in December 2013.

We disclose that our policy director, Javier Ruiz, is also a member of the Quality Assurance group that will examine the responses to the consultation.

The Cabinet Office is embarked on an attempt to redesign public administration, a new digital revolution led by a belief in the power of data to solve every problem. We've often heard arguments that if Google can do this or that, why can't the government. This needs some pause. At ORG we also believe that we are at the gates of a data revolution, but unless we put people squarely at the helm this may not lead to the positive outcomes data evangelists expect. This is a highly sensitive area for privacy campaigners.

We have listened carefully for the arguments as to why the government wants make data sharing between public bodies - and a few private entities - easier and faster. Our instinctive response as privacy advocates is that removing friction and barriers could also remove controls and enable the proliferation of invasive databases. For example, removing the need for Parliament to approve new data flows - a key plank of the proposals - speeds up the process considerably. It also removes public accountability.

The critical question in this process is whether it is possible to have agile and fast data flows within government to quickly match policy developments while providing adequate protections and avoiding a free for all. It may be possible to make some improvements, but this cannot involve removing all democratic controls.

We know that despite our best efforts in the Open Policy Making process the end result will not be exactly what we would have liked. We remain positive about the engagement though, as it has sharpened our capacity to constructively intervene in policy making, and many details in the proposals have been improved. We expect that wider scrutiny under the consultation will find loopholes we may have missed.

As many of our specific objections and concerns have already been dealt with, this makes it all the more important to explain very clearly our remaining reservations about the overall approach and specific areas.

One difficult issue for us throughout the process has been to focus our engagement on privacy and data aspects, not straying too far from our core issues. At the same time, as part of civil society representing a public interest position, we've had to raise broader points on the fairness of the underlying policies. Where possible we've brought along other organisations with expertise in particular areas such as debt.

This approach should continue and be expanded to other strands such as public service delivery.

Our principles

ORG's minimal criteria are that data sharing agreements should not lead to a widespread intrusion on people's privacy; should be proportionate, limited in scope and enshrine fundamental rights; and carry strong safeguards against wilful abuse and unintended consequences.

It would be fair to say that these aspects have been taken very seriously by the Cabinet Office team and particularly the scope of proposals has been tightened. We are concerned however that in cases safeguards are placed in codes of practice, which are no substitute for primary legislation.

One concern around safeguards is the tendency throughout the process to see compliance with data protection laws as a safeguard. We have stressed that this is not necessarily the case. This is particularly problematic with the new EU General Data Protection Regulation (GDPR), which is set to replace the Data Protection Act as the backbone of privacy protections in the UK. The recently approved GDPR is a much needed update and an overall improvement, but during a long and convoluted negotiation process European governments carved out many exceptions in the GDPR that give public administrations plenty of room to manoeuvre around privacy restrictions. Data sharing legislation needs to provide specific safeguards closing any potential loopholes.

More proactively, ORG engaged in this process as an opportunity to consider the expectations and relationships between citizens and government. Putting citizens at the centre of a new data-driven administration should include devolving much higher levels of control to individuals. It is disappointing that these aspects have not been explored.

Where devolving control is not possible - e.g. taxation or justice - new information governance models need to accompany any increase in data sharing. We have concerns that simply creating a legal powers without a shift on how we see personal information could end up taking us to widespread data sharing without any consent.

At the very least this legislative drive could be an opportunity to streamline the vast number of data gateways currently in existence and improve transparency. Where the Cabinet Office sees an administration hamstrung by restrictive privacy regulations, we refer them back to the Joseph Rowntree sponsored report from 2009, which found large numbers of government databases had problems and some may well be in breach of human rights laws.

The proposals contain some improvements on transparency, and a rationalisation of data flows has been a subtext to much of the discussions, but we believe these are not enough. We would like to see mandatory central registers of data transfers and the closure of "zombie" sharing agreements when new ones are started. Use it or lose it sunset clauses should become the norm in any new data agreement.

Accountability is also paramount. If Parliament is not to have a role in authorising data sharing we need to have mechanisms for challenging any new agreements without the need to go to court for a judicial review.

Safeguards should be included on the face of the bill if possible and only in codes of practice if they need detail or may need to be modified frequently. There is no reason not to include almost any safeguards in the bill itself.

It is unclear what legal obligations public bodies will have with regards to the codes and in most cases non-compliance does not even lead to automatic disqualification from data agreements.

Increasing data sharing may bring some improvements to government efficiency and the quality of public policy, but the case for these positive outcomes, given the other costs, must be clearly made. The criteria for success must be clear. Ultimately government must demonstrate that from a human rights perspective the privacy intrusion is proportionate to the public interest objectives.

Throughout the discussions we also found a healthy scepticism among some civil servants, who believed that there were other issues that would need to be tackled besides legal powers, such as technical capacity and organisational culture. These issues are barely mentioned in the consultation but came up repeatedly during the open policy making discussions.

The proposed strands and overall concerns

We will go in more detail below but here we want to give a quick summary of our views on the concrete proposals included in the legislation.

The proposals around research and statistics are the least problematic from our perspective. If safeguards are applied properly sharing data for these purposes could lead to better policies and insights without causing disproportionate privacy intrusions.

The proposals on fraud are sensitive because there is a thin line separating it from errors. Indeed, during the discussions with the Cabinet Office we looked at the use of data to reduce administrative errors and prevent fraud as part of the same processes. Here our main concern is on the review and the removal of the sunset clause.

The third strand on profiling for public services is one area where we see very high risks. There are dangers of discrimination, stigma, and risk aversion leading to oversensitive reactions. Safeguards and ensuring the non punitive character of the measures needs to be very tight and the proposals can be improved.

One common thread is the central role of HMRC's data, with many of the provisions in the proposals designed to remove statutory limitations on access. The wider implications of these changes should be debated more widely. It is true that there was a previous consultation, but we would like to see a summary of all the changes proposed around HMRC to get the full picture.

Health data will not be part of this process until the Caldecott review. We will expect a high degree of engagement when proposals are added to the contents of this consultation.

Our main concerns centre on the two proposals that have been brought into the process very late and we think should be simply removed. These are very controversial, and go against the grain of the process, which was designed to find the areas where agreement could be found.

We are worried about proposals to share data on debt that were removed and then brought back at the end of the Open Policy Making process. The proposals to enable widespread data sharing to tackle government debt have not been supported by a

clear case, and could have huge implications for vulnerable people facing economic hardship. Creating a “single view of debtors” requires a broader strategy on public debt management that is currently missing. As such we think it would be best to leave these proposals out of the current process and take more time to consider the issue of debt as a whole, not just the data angle.

Another last minute addition is the plan for the sharing across government of data from the General Registry Office. We can see the case for making it easier to for citizens to send certificates electronically instead of having to apply and send a paper copy by post. In contrast we have severe concerns about proposals for bulk sharing of the whole registry database across government to improve identification. Despite repeated reassurance to the contrary, the sharing of these common identifiers across government has a whiff of ID Cards lite. In cases where bulk registry data might be useful, such as fraud prevention, specific agreements should be explicitly mandated by Parliament, instead of creating a broad power.

In any case, bringing such proposals into this process late runs against the spirit and intention of the open policy process. Government should remove them, if only to retain the credibility of future processes. If they are retained, then civil society will take note, and be far less willing to engage in such processes in the future. There is, in short, an element of good faith which is being sacrificed here.

Improving public service delivery

General comments

The proposals ask for flexibility in exchange of safeguards. The safeguards need to be as strong as the powers of the ministers to act without Parliament.

Our general concern in this section is that safeguards need to be made more explicit in the bill itself.

Changes to the objectives covered in the bill should allow for proper discussion and modifications by Parliament.

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

YES

Our concern is that while the intention is good, the wording “individuals of a particular description” may not reflect the dynamic nature of the proposed measures. The data may well define whether individuals are in or out of the programme, e.g. they are “troubled families”, and it is about the criteria being used, not an intrinsic quality of the individuals affected. Our understanding is that it should not be about labelling people.

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

YES

The inclusion of police forces appears to counter the stated objectives of focusing on welfare. Combined with the clauses allowing for the use of data for criminal investigations this is concerning.

In general the proposed schedule is very broad. E.g. It is unclear why the Duchy of Lancaster needs the power.

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

Strongly disagree

Private entities should not included by default in the schedule. There are other mechanisms for data sharing, for example as part of the delivery of a contract, that would allow the required information to be accessed if needed.

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

Disagree

Codes of Practice have to be explicitly consistent with GDPR requirements.

There is need to explain the need to have a specific voluntary Codes of Practice when there are Statutory Code of Practice on data sharing. How will these interact?

There is a risk that the Codes of Practice are modified to be made too weak; the ICO should be able to veto any Code of Practice.

The principles for the code of practice should be included on the face of the bill: the need to provide a case, safeguards, transparency. (See below form consultation document). The code needs to spell these out in detail.

"It is proposed that the Code for the public service delivery power will specifically include the following sections:

- a. Principles for use of the power. This would include details on when the power is intended to be used;*
- b. Guidance for successful implementation. This would include details such as what a business case for data sharing under the power should cover and best practice examples; and*
- c. Additional safeguards. This would include details of additional safeguards, such as the requirement to publish Privacy Impact Assessments. These supplement the safeguards which have been built into the in the power itself (such as the permissive nature of the power) as well as those in existing legislation, such as the DPA."*

Basic safeguards, such as restrictions on the reuse of the data for other purposes under statutory powers of the body involved, should be mentioned in the bill and fleshed out in the codes.

The basic transparency criteria is the need to keep a public record of data agreements made under the provisions . This should be in the bill, not in the code.

The bill should establish set periods of reviewing the code of practice, not “from time to time”.

Additional issues not raised in the questions

The consultation document sets out clear criteria for the use of the power which have been subjected to long discussions:

“The proposed power is intended for use in situations where:
a. The objective could not be met without data sharing;
b. 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 making; and
c. Sharing and analysis of de-identified data would not achieve the intended outcome.”

These should be reflected in the legislation, possibly in part 7, which is not the case now. Then expanded in the code.

Even with best intentions people can be stigmatised or may simply not wish to participate. Individuals need to be able to opt out from participation and profiling as much as possible. Government should publish more details to explain why and how data sharing is consistent with A.8 ECHR when data sharing proceeds in the absence of data subject consent.

The draft clauses attempt to define “personal information”, but this should probably be referred to data protection law to avoid inconsistencies.

Extending the provisions to new objectives can be done by ministers through Statutory Instruments. It is critical in order to future proof the legislation that amendments to the SI can be made as part of the affirmative resolution procedure.

Draft clauses 2(2) allowing the use of information contain provisions for criminal investigations, emergencies, safeguarding and national security that are too broad. Police and other bodies included in the schedule could use this data sharing agreement to bypass other procedures. HMRC data is exempted from these clauses, so why not other data?

The proposals do to take into account that in most cases data flows will go in one direction only. Legislation needs to set out clearer responsibilities for the originator

and the receiver of the data. In some cases the legal status may be different if the receivers of data are only processing the data on behalf of other public bodies.

Providing assistance to citizens living in fuel poverty

General comments:

We support the proposals provided the principles set out in the consultation are adhered to.

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

Agree

We agree that energy providers should be told about people who qualify for assistance but will not be given access to the underlying data used to do the matching.

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

N/A

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

Access to civil registration to improve public service delivery

N/A

Increasing access to civil registration information to improve public service delivery

General comments:

E-government access to individual certificates can be positive, but we think bulk sharing should not take place.

We are extremely concerned about the bulk sharing proposals and will campaign to oppose them.

The bulk proposals are tantamount to an ID card lite and we are certain that will be rejected by public opinion, as previous attempts have been in the past.

The Conservative Party in opposition was against ID cards and would need to explain in Parliament why they have reversed their position in Government.

The proposals do not fit the principles agreed in the open policy making process: “no indiscriminate sharing of data within Government;”. Adding bulk sharing to the open policy making framework brings the whole process into disrepute.

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

Neither agree nor disagree

This could be positive in principle, but should only take place with the consent of the individual involved.

If done properly it is unclear why this could not be extended to marriage and death certificates.

Paper based alternatives should be maintained.

The relationship of this proposal with the Verify identity assurance programme needs to be explained.

Given the low costs of marginal copies of certificates fees for electronic certificates should be based on independently agreed calculations.

There are many issues with the breadth and quality of the digital General Register database that we believe should be solved before embarking on major legislative changes.

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

Strongly disagree

The consultation paper states: “During open policy-making discussions, concerns were raised that the proposed new powers would create a citizen database.” The

Data sharing consultation ORG

concern raised and confirmed by the consultation documents is about the generalised use of common identifiers across government. We understand that the proposals will not create a new “citizen database”, but will enable widespread data matching in England and Wales, with a form of “ID card lite”. The core principle of ID is not the card itself but the unicity of the number or key and the centralisation aspects.

This would be a major departure from established custom and practice in the UK. The consultation states that : “Acts of Parliament governing civil registration are out-dated, primarily the Births and Deaths registration Act 1953, the Registration Service Act 1953, and the Marriage Act 1949”.

If anything this shows how inimical these proposals are to the status quo and the need for broader reform and discussions, rather than attempting to sneak in the proposals at the last minute and in a different context.

The consultation goes on to say: “Where no such statutory gateway exists, information cannot be shared”. The proposals would completely reverse the situation by creating a generalised and unconstrained power “to assist public authorities to fulfil their functions”. Access to GR data should be clearly limited to specific purposes agreed by Parliament.

The draft legislative clauses presented do not contain any limitations or safeguards, with any such considerations referred to a future code of practice prepared by the Registrar General for England and Wales in consultation with Information Commissioner. This is not sufficient.

The security aspects of bulk sharing have not been properly explored in the consultation. There is mention of reducing identity theft through the use of electronic certificates instead of paper copies, but the risks associated with sharing the data across government are not discussed.

Combating fraud against the public sector through faster and simpler access to data

General comments:

Fraud investigations can be a legitimate use of data sharing, if done narrowly and proportionately and without wholesale data matching.

These proposals contain considerable detail and have clearly been thought through. Unfortunately, in our view they still need more work.

Our main area of concern is the review of the powers and the apparent lack of Parliamentary, abandoning the sunset approach.

Other issues:

It is positive that the proposed new power is centred on enabling pilot projects to test ways of preventing and combating fraud against the public sector. It is unclear however, how this will be enforced in the legislation.

The Government proposes to extend the power to private organisations that provide services to a public authority. As a safeguard the proposed legislation limits that these types of bodies can only use the data for the function that it exercises for a public authority. We are not sure why the general power needs to be extended in such a manner and these situations cannot be dealt with as part of the contracts for service delivery. This needs to be explained, as in principle we would be opposed to this.

The drafting of the powers in the clauses is too broad, potentially allowing any data to be ingested by public bodies for fraud purposes.

The draft clauses include very different activities. Our understanding was that the programme was about prevention, detection and investigation of fraud. The actual draft clauses include: "prosecuting fraud of that kind; bringing civil proceedings as a result of fraud of that kind; taking administrative action as a result of fraud of that kind". Once that fraud has been confirmed we would expect that normal procedures would take over. Extending the power to prosecutions and enforcement is very different and needs more consideration and better explanation.

The proposals on fraud are sensitive because there is a thin line separating it from errors, ultimately the intention involved. Indeed, during the discussions with the Cabinet Office we looked at the use of data to reduce administrative errors and prevent fraud as part of the same processes. Error is now not mentioned except in passing, and Government should explain why.

More generally, there is a wider public policy debate as to the focus of fraud investigations, and whether small scale fraud by ordinary people, sole traders and small businesses is disproportionately targeted in relation to tax avoidance by high net worth individuals and corporations. In the three years since we started looking at these proposals the social climate and potential legitimacy of such measures have changed substantially.

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

Yes

More safeguards and limitations in scope should be set out in the bill, and expanded in the code.

The draft clauses have limitations on sensitive data (race, religion, trade union membership...). It would be simpler to refer to data protection law to avoid potential inconsistencies.

Draft clause 3(2)a allows for the disclosure of data “which is required or permitted by any enactment” and the next clause if it “is required by an EU obligation”. These exemptions are too broad and could make any safeguards practically useless. The clause does not apply to HMRC data.

To ensure that the disclosure of data under this power is consistent with the Data Protection Act 1998, it is proposed that the legislation explicitly states that data cannot be disclosed under the new power if it contravenes the DPA or Part 1 of the Regulation of Investigatory Powers Act 2000. This may not be enough, and both legislations are in the process of being superseded. More specific safeguards should be provided.

A definition of personal information for the purpose of the power is included in the legislation, covering legal persons. The relationship to data protection - covering natural persons - needs to be clarified.

It is positive to see a proposed Strategic Steering Group which would include representatives from Government, interested Civil Society Organisations and independent observers.

We broadly support the proposed three stage process, moving from validation to light analytics, to detailed analytics. However, although it is true that at each stage the number of people under consideration would be reduced, the richness of the data would increase and new safeguards should be triggered.

The proposed principles for the Code of Practice are sound, but there is no reason not to mention some of them in primary legislation:

- 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 data disclosures once the power is commenced;*
- c. all participating organisations must periodically publish the measurement data coming from the data sharing arrangements; and*
- d. all recommendations of the Strategic Steering Group being published and made available online.*

Transparency over the data sharing is important, although we understand concerns about hindering enforcement by tipping off would be fraudsters. It would be important that impact assessments and other documents are detailed enough to allow proper scrutiny.

11. It is proposed that the power to improve access to information by public authorities to combat fraud will be reviewed by the Minister after a defined period of time. This time will allow for pilots to be established and outcomes and benefits evaluated. How long should the Fraud gateway be operational for before it is reviewed?

It is proposed that the power be reviewed three years after it comes into force, with a decision then taken whether to amend or repeal the power. Criteria for reviewing the

power would be published by the relevant Minister. It is proposed that the review itself would be carried out in consultation with the Information Commissioner's Office and other appropriate persons and the results published and laid before Parliament.

We do not have a view on the best time period but it should enable proper assessment. It would be better to have a longer period than rush an incomplete review.

We are very concerned about moving away from a sunset clause, which was the view taken during the open policy-making discussions. We do not believe that carrying out a review and then providing the relevant Minister the option to repeal the legislation is an equivalent safeguard against potential future abuse. There is very little evidence of legislation ever being repealed in such a manner.

We can see the attractiveness of avoiding the need to reintroduce the powers in primary legislation if the powers proved to be effective; but not at the cost of abandoning Parliamentary approval. We don't agree that "the approach taken in the proposed legislation is consistent with the spirit of what was agreed during the open policy-making process".

The decision to continue with the legislation should not fall to the Minister but Parliament. Interim procedures or some other solutions would need to be found to ensure that what is working is not abandoned.

Here, as in the rest of the data sharing process, we must find the balance between flexibility and protection of rights. The document makes this clear when stating that the current numerous express gateways on fraud have been designed "to be specific to ensure a smooth passage through parliament". We must be careful that the process does not appear to bypass future democratic controls.

The successful completion of the pilot period would not simply trigger the extension of the powers, but also their expansion from pilots into wider use. Surely this will need to be discussed and agreed.

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

General comments:

We are particularly worried about proposals to share data on debt that were removed and then brought back at the end of the Open Policy Making process.

The proposals to enable widespread data sharing to tackle government debt have not been supported by a clear case, and could have huge implications for vulnerable people facing economic hardship.

Creating a "single view of debtors", as recommended by the National Audit Office in its 2014 report 'Managing Debt Owed to Central Government', requires a broader

strategy on public debt management that is currently missing. The proposals might enable better handling of hardship, and /or prioritisation of debt, but these processes simply do not exist and have not been openly discussed by Government as part of the process.

If Government has plans for centralising debt management, they should be more candid about them. Proposing changes to data sharing in a vacuum of related policy is not acceptable. As such we think it would be best to leave these proposals out of the current process and take more time to consider the issue of debt as a whole, not just the data angle.

The consultation complains about the 86 data gateways around debt, but there is nothing in the proposals explaining how the new powers would help rationalise this situation and not simply increase the number of available channels.

The proposals do not contain any projections of the expected reduction of debt, or any other consideration of the proportionality of the huge privacy intrusions being proposed here. This leaves them open to legal challenges.

The consultation includes various case studies of how data sharing is currently used in bilateral agreements around debt. One example involves the Student Loans Company sharing data with DWP and HMRC to establish eligibility to make repayments. This is very different from the centralised view of debt presented elsewhere and makes it very confusing to understand what Government really wants, other than a carte blanche to try anything they wish in the future.

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

N/A

13. How can Government ensure the appropriate scrutiny so pilots under the power are effectively designed and deliver against the objectives of the power?

The proposed clauses are almost identical to those proposed around fraud. The references to pilots are only superficially treated in the consultation document in contrast to the level of detail provided around fraud.

The powers as they stand could be used to recover private sector debt, as a "specified person" includes those providing a service to public bodies. We hope this is an unintended mistake, but as we said in relation to public services the proposals in general do not make enough distinction on the flows of data.

There are some positive ideas for the code of practice that would limit the scope of the proposals, but in this context they are not enough.

14. It is proposed that the power to improve access to information by public authorities for the purpose of better managing debt owed to government will be reviewed by the Minister after a defined period of time. This time will allow for pilots to be established and outcomes and benefits evaluated. How long should the debt power be operational for before it is reviewed?

We have similar concerns as those expressed around the fraud proposals.

In this strand it would be even more critical to ensure a sunset clause is in place if a bill was presented to Parliament, given the lack of clarity.

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

General comments:

We are broadly supportive of the proposals if implemented properly with adequate safeguards.

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

NO

We are opposed to fees because they commercialise the exchange and undermine the principle to make research publicly accessible. If private institutions “pay” for data this destroys the quid pro quo to bring back the benefits of research to the public.

The public sector organisations that happen to hold data about citizens are not the same as “the public” and they should not be the exclusive beneficiaries.

Any fees should ensure that public interest projects with limited funding are not disadvantaged by commercial organisations.

Very strict marginal cost recovery should be applied to stop public bodies from overcharging for data they have created in the course of performing their Public Task.

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

YES

This would help future applicants and it is basic good practice.

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

As discussed during the open policy making process it would be important to ensure that the results of research that relies on public data are openly accessible.

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

General comments:

We are broadly supportive of the proposals if implemented properly with adequate safeguards.

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

N/A

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

- (a) the administration burden experienced and the costs incurred in completing the survey, and
- (b) ways in which the UK Statistics Authority should seek to use the new powers to further reduce the administrative burdens on businesses who provide data to the ONS for the purposes of producing National and other official statistics.

N/A

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

Given the attention given to these legislative proposals it is surprising how little the consultation contains on safeguards and the code of practice.

While we generally trust the Statistics Authority to handle data properly, it would be good to see more detail, particularly on data requested from the private sector.

In particular data from mobile companies, social media or other such sources such as smart meters or sensors in smart cities need special consideration, with data subjects affected being given enough information.

Data sharing consultation ORG

In some cases, the Statistical Authority will be able to combine data sources and re-identify databases that have previously been declared non-personal information and out of data protection.