Cabinet Office

Digital Economy Bill: Digital Government (Part 5)

Introduction to Data Sharing Codes of Practice

The most successful technology businesses are adept at using data to drive improvements for their customers. Used responsibly, and with the right safeguards, government could use data to deliver radically better public services and save money. The Digital Economy Bill contains a suite of measures that will support the digital transformation of government, enabling the delivery of better public services, world-leading research and better statistics.

Part 5 of the Bill, which deals with Digital Government, sets out provisions to enable the disclosure and sharing of data for specified purposes. These provisions include a set of permissive gateways designed to enable more effective and efficient sharing of data between specified bodies for particular purposes, with a view to fulfilling specific objectives. For example, the powers will help public authorities identify individuals or households who are eligible for specific types of support and services and ensure they are offered at the point of need.

The measures provide new permissive powers for public authorities to share information to combat fraud against the public sector. Public authorities will be empowered to pilot new ways of using data to improve the management of debt owed to the public sector by reducing the time and complexity involved in establishing data sharing agreements. Where a vulnerable customer is identified, the intention is that the sharing of data for this purpose might enable that person to be given appropriate support and advice, which may include signposting to non-fee paying debt advice agencies.

The UK Statistics Authority will be given easier secure access to data to produce more timely and accurate national and official statistics. Researchers will be provided with a more complete and accurate evidence base to inform analysis and enable better policy design and delivery.

These provisions are intended to simplify a complex legal landscape and unlock the potential of publicly held databases to improve the lives of citizens. Increasing citizens' confidence in the government's use of their data while making better use of

that data to deliver services they need will help us to build a more prosperous society. Information sharing under the powers must comply with the Data Protection Act (DPA). Information can only be shared for specific purposes. In alignment with the DPA, public authorities will as a matter of principle use the minimum amount of information required. The use of canonical datasets by public authorities will support this.

We are publishing the four codes of practice that will give practitioners and citizens clarity and transparency over how the powers in the Bill will operate. They cover:

- A code of practice on Public Service Delivery, Fraud and Debt (Chapters 1, 3 and 4)
- A code of practice for civil registration officials (Chapter 2)
- A code of practice and accreditation criteria for access to data for research purposes (Chapter 5)
- A statement of principles and procedures and code of practice for changes to data systems (Chapter 7)

Our codes are drawn from, and should be read in accordance with the Information Commissioner's Office (ICO) code of practice on data sharing, which provides the framework for how the DPA applies to the sharing of personal data. Our codes also include guidance on the development of privacy impact assessments and privacy notices, again drawn from ICO codes.

Cabinet Office
19 October 2016

Cabinet Office

Data Sharing Code of Practice

Code of Practice for public authorities disclosing information under chapters 1, 3 and 4 of the Digital Economy Act [2017]

Date: 19 October 2016

Produced by Cabinet Office

Contents

Part 1: About the Code of Practice

1. This Code explains how the permissive powers contained in Chapters 1, 3 and 4 of Part 5 of the Digital Economy Bill should be used for the sharing of information by officials within specified public authorities for specific purposes set out in the legislation or, where appropriate, accompanying regulations. It also makes reference to requirements under the wider UK legislative framework, where appropriate. In addition, it provides details of the procedures that need to be followed when considering the disclosure, receipt or use of information under the powers. This Code should be read alongside the Information Commissioner's data sharing code of practice ('the ICO Code') which provides guidance on how to ensure personal data is shared in a way that is lawful, proportionate and compatible with the Data Protection Act 1998 (DPA) and other relevant legislation such as the Human Rights Act 1998.

2. This Code defines 'data sharing' in the same terms as the ICO Code[1], namely the disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. The ICO Code states that data sharing can take different forms including:

    - a reciprocal exchange of data;
    - one or more organisations providing data to a third party or parties; and
    - several organisations pooling information and making it available to each other.

3. The relevant chapters of Part 5 of the Digital Economy Bill (i.e. pertaining to public service delivery, debt and fraud) define personal information as information which relates to and identifies a particular person (or body corporate)[2]. For these purposes, information 'identifies' a particular person if the identity of that person is (a) specified in the information; (b) can be deduced from the information, or (c) can be deduced from the information taken together with any other available information. The Data Protection Act 1998 ('DPA') defines personal data rather than personal information. Personal data for the purposes of the DPA is defined as data which relates to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of the data controller. The definition for the purposes of the DPA also includes the expressions of opinions about an individual and the indication of intentions around that individual.

[1] https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf
[2] the definition of personal information does not include information about the internal administrative arrangements of the specified body permitted to disclose or receive data under these permissive powers.

4. The definitions of ‘personal information’ contained in the Bill are intended to ensure that the information shared through these powers is handled carefully. Though the definition of ‘personal information’ for the purposes of the Bill may differ from the definition of ‘personal data’ in the DPA, all information shared and used under the public service delivery, debt and fraud provisions must be handled in accordance with the framework of rules set out in the DPA, and in particular with the Data Protection Principles. There are also specific safeguards introduced in the Bill to ensure personal information is handled appropriately.

5. The public service delivery, debt and fraud provisions are subject to the DPA, including the criminal offences in relation to the unlawful obtaining or disclosing of personal data set out at section 55. New criminal offences have also been created to prevent the unlawful disclosure of personal information. Individuals convicted under those offences could face a maximum penalty of up to two years in prison, an unlimited fine, or both. These maximum penalties mirror those applying to existing offences contained in legislation governing the use of data held by HMRC and DWP, and are designed to underline the Government’s commitment to protecting citizens’ data.

6. In the past data sharing has commonly involved bulk data transfers within and between public authorities. New technology and methods have had a significant impact on data sharing. Application Programming Interfaces (APIs) are standards that allow software components to interact and exchange data. APIs allow applications and their datasets to interact with each other across organisational and geographical boundaries. This allows public authorities to identify or verify eligibility for services and other objectives for which data needs to be shared through less intrusive methods, such as running binary checks against one or more datasets. Though the method is generally safer (large amounts of data are not being transferred either physically or electronically and, in instances when eligibility is being checked, the need to share underlying data is removed completely) and less intrusive (binary checks can be run against very specific relevant data fields) information is still being shared and as such those sharing data in these ways require the legal powers, to do so.

7. In light of the fact that we are in transition between old and new approaches to data sharing, the legislation is intended to support the range of different approaches to data sharing and as such does not specify the use of a particular technology or a specific approach to be used in terms of the practicalities of transfer. Furthermore, we recognise the need to allow the opportunity to keep apace of and adopt better technologies and more efficient or effective approaches as they emerge.

8. The Government Digital Service (GDS), which is a team within the Cabinet Office leading the digital transformation of government, continues to work on how best to transition public authorities from outmoded legacy systems to the technologies required for a modern public sector. Future revisions to the Code

may reference or include guidance and best practice in relation to technical processes.

9. This Code does not provide guidance on individual organisations and their obligations on data sharing or data handling. Instead, in making use of these powers, you will need to satisfy yourself that you are complying with the DPA. It is advisable for those making use of the powers to seek your own legal advice regarding data sharing following any agreements to share information.

The Code's status

[This is indicative text to be added in the final version following formal consultation]

10. The Minister for the Constitution, Cabinet Office, has prepared and published this Code under section 35 of Chapter 1 (public service delivery), section 44 of Chapter 3 (debt owed to the public sector) and section 52 of Chapter 4 (fraud against the public sector) of Part 5 of the Digital Economy Bill. It has been developed in consultation with the Information Commissioner's Office, Ministers within the Devolved Administrations, as well as other relevant persons and has been laid before the UK Parliament and the devolved legislatures in Scotland, Wales and Northern Ireland, in accordance with the duties set out in the Act.

11. The contents of this Code are not legally binding, though the provisions of the Bill require that you have regard to the Code when making use of these powers. The Code does not itself impose additional legal obligations on parties seeking to make use of the powers, nor is it an authoritative statement of the law. It recommends good practice to follow when exercising the powers set out in the Bill. Government departments will expect public authorities wishing to participate in a data sharing arrangement to agree to adhere to the code before data is shared. Failure to have regard to the Code may result in your public authority or organisation being removed from the relevant regulations and losing the ability to disclose, receive and use information under the powers.

Who should use the Code?

12. All persons responsible for or working in a capacity where they have to consider sharing information under chapters 1, 3 and 4 of Part 5 of the Digital Economy Bill must have regard to this Code and should include a statement of compliance within any data sharing agreement produced under the powers.

13. Public authorities able to make use of these powers are set out in regulations which can be found at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535311/2016-07-05_Digital_Government__Disclosure_of_Information__draft_regs.pdf

Part 2: Understanding the public service delivery, debt and fraud powers

Purpose of the public service delivery power

14. Public service delivery is changing, due to increasing acknowledgement that services are more efficient and effective when they are joined up. Joining up services requires sharing of data. This is presently hampered by a lack of clear and robust legal gateways which public authorities are confident will enable them to share relevant data on the individuals and families they are working with in compliance with the DPA. The primary purpose of the power is to support the well-being of individuals and households. Data sharing arrangements cannot be established for purposes which are to the detriment of the individual or household.

15. Three specific objectives for which information can be disclosed under the power will be set out in regulations. Further objectives can be added through regulations by an appropriate Minister in HM Government or in the Devolved Administrations. The objectives that have been drafted in regulations so far are:

- Identifying and supporting individuals or households who face multiple disadvantages and enabling the improvement or targeting of public services to such individuals or households and providing for the monitoring and evaluation of programmes and initiatives';
- Identifying, making contact with and establishing the entitlement of individuals and households who might need assistance in dealing with changes to use of any part of the electromagnetic spectrum between 470-790 MHz following the 700Mhz band being cleared for mobile broadband use;
- Reducing the energy costs, improving efficiency in use of energy or improving the health or financial well-being of, people living in fuel poverty.

16. The first objective around supporting individuals or households who face multiple disadvantages is designed to support those programmes and initiatives where different public authorities and other bodies need to work together to support vulnerable individuals and families, such as delivery of the Government's Troubled Families programme. Multiple disadvantages can be interpreted broadly as social and economic factors, which includes education, health and financial problems.

17. The second objective that is drafted in regulations allows data to be shared by DWP and other public authorities in order to identify vulnerable people who might need help from the authorities in re-tuning televisions in 2018/19 after the 700Mhz band will be used for mobile broadband rather than to transmit digital TV. Whilst it is expected that many of those affected can be identified through a consent-based approach, some individuals may be reluctant to identify themselves as being in need of support. This power will help to identify those who are most in need of support. Details of how the scheme will operate are being developed, but secure management of data will be a key requirement for all those who process it.

18. The third objective that is drafted in regulations allows data to be shared by specified public authorities for the purposes of reducing the energy costs, improving efficiency in use of energy or improving the health or financial well-being of people living in fuel poverty.

19. For the purposes of this legislation, a person is to be regarded as ″living in fuel poverty″ if they are a member of a household living on a lower income in a home which cannot be kept warm at reasonable cost. Schemes for providing assistance to persons living in fuel poverty may be run by public authorities, such as local authority or government run grant schemes, or they may take the form of supplier obligations, like the Energy Company Obligation (which was made under various provisions of the Gas Act 1986 and the Electricity Act 1989) and the Warm Home Discount (which was made under Part 2 of the Energy Act 2010), where the assistance is delivered or promoted by energy suppliers.

20. The best way to guarantee that this assistance reaches those who need it is to provide it automatically, although automatic rebates can only happen if the state can inform energy companies which of their customers should receive it. Pensioner households already receive rebates in this way, because a specific data sharing gateway has been created in section 142 of the Pensions Act 2008 to enable it to happen. This has been used to enable electricity suppliers to automatically provide rebates to customers on state pension credit under the Warm Home Discount scheme, without the need for the customers to identify themselves by applying for support. The data sharing gateway provided by this Bill is intended to be used in a similar way for other vulnerable persons.

21. A number of different public authorities hold data about incomes and dwelling characteristics, which would enable better targeting of fuel poverty support schemes at those in greatest need and more efficient delivery of the assistance to people living in fuel poverty.

22. The regulations will describe the objective as:
    - assisting people living in fuel poverty by reducing their energy costs,
    - assisting people living in fuel poverty by improving efficiency in their use of energy, or

- assisting people living in fuel poverty by improving their health or financial well-being.

23. Any disclosure of information to gas and electricity suppliers must also be for the purpose of reducing the energy costs, improving energy efficiency or the health or financial well-being of people living in fuel poverty and it must be disclosed for use in connection with an energy supplier obligation scheme. These schemes are the Warm Home Discount and the Energy Company Obligation. This enables other datasets to be used for the purpose of providing support under the Warm Home Discount and Energy Company Obligation schemes to people living in fuel poverty. Amendments can be made by affirmative regulations to the list of support schemes for which the information may be disclosed and to the list of permitted recipients of the information.

24. The purpose of the disclosure must always be to assist people living in fuel poverty.

25. In general, information disclosed under the power can only be used for the purposes for which it was disclosed. There are very limited instances where you can use information for another purpose. These circumstances are specifically:

- If the information has already been lawfully placed into the public domain;
- If the data subject has consented to the information being used for another purpose;
- For the purpose of a criminal investigation;
- For the purpose of legal proceedings;
- For the purposes of preventing serious physical harm to a person and loss of human life, safeguarding vulnerable adults or children, responding to an emergency or protecting national security.

26. These provisions do not apply to personal information disclosed by HMRC, which includes the Valuation Office Agency (VOA). Personal information which is disclosed by HMRC is subject to special protections, which reflect the confidentiality of HMRC information and the trust and confidence in which HMRC holds information, and so personal information disclosed by HMRC may not be used for other purposes, unless with HMRC consent. The criminal offence for wrongful disclosure of HMRC information continues to apply to HMRC information in the hands of the recipient.

The process for establishing a new objective under the public service delivery power

25. The public service delivery power has been designed to give you the ability to respond more efficiently and effectively to the data you need to address emerging social and economic problems. The power allows Ministers in the UK

Government and Devolved Administrations (for devolved matters) to add new objectives via regulations. New objectives must meet the following two conditions set out in primary legislation:

- The objective has as its purpose -
    - the improvement or targeting of a public service provided to individuals or households, or
    - the facilitation of the provision of a benefit (whether or not financial) to individuals or households.

- The objective has as its purpose the improvement of the well-being of individuals or households. The well-being of individuals or households includes their physical and mental health and emotional well-being, the contribution made by them to society, and their social and economic well-being.

26. The intended interpretation of 'benefit' in the first condition is the offer or delivery of a service or intervention or type of financial assistance that is for the good or advantage for the individual and their family. Although an individual may not recognise that there are issues that need to be addressed, for example in some cases of alcohol or drugs dependency, the defining of benefit should be consistent with Government social policy and ensuring the well-being of the individual.

27. "Well-being" is a broad concept, and for the purposes of these provisions relates to areas such as social and economic well-being, the individual's contribution to society, or their participation in work, education, training or recreation, suitability of living accommodation, physical and mental health and emotional well-being, protection from abuse and neglect, control of the individual over their day-to-day life, and positive domestic, family and personal relationships.

28. If you wish to propose to add a new objective you will first need to determine what types of data are required, which bodies hold the data and how the ability to share personal data will support achieving your policy objectives. Objectives should be drafted to ensure that they are aligned to conditions in primary legislation and specific enough to constrain the use of the power to a clear purpose. Where an objective has been developed by a devolved administration for a specific devolved matter, the objective should specify that it relates to a specific devolved territory.

29. Objectives must be sufficiently specific that they identify a section of the population and *what the intended benefit to some individuals* from that target population is. This can be identified in the form of one or more outcomes, all of which fit into the field of social policy.

Example objectives

Example of potentially suitable objectives are:

1. Reducing the number of people sleeping on the street for more than one night;
2. Improving employment outcomes for ex-offenders; and
3. Supporting gang members to safely exit gang culture.

Examples of objectives which would not meet the criteria because the objective is punitive are:

1. Identifying individuals operating in the grey economy; and
2. Identifying welfare claimants erroneously receiving welfare benefits.

Examples of objectives which would not meet the criteria because they are too 'General' in terms of targeting communities or broad public benefit rather than individuals or households or so broad that almost any data sharing arrangements could be enabled under it include:

1. Improving levels of safety in a neighbourhood;
2. Helping people into work; and
3. Preventing people going to prison.

30. You should discuss your proposal for a new objective with the relevant central government body with oversight responsibility for the respective policy area to seek their views. Either your organisation or the responsible central government departments can write to the Minister for the Cabinet Office and request for the new objective to be added via regulations. Once the Minister has agreed to the creation of a new objective, consultation must take place with the Information Commissioner's Office, relevant Ministers from the devolved administrations, Commissioners for HM Revenue and Customs and other persons as the Minister considers appropriate.

31. Public authorities within a devolved territory proposing to create a new objective limited to a devolved function involving devolved bodies within that territory should contact the relevant Ministerial body in the devolved administration (e.g. the Department of Finance in Northern Ireland). Ministers within the devolved administration have the powers to make regulations to create objectives within the legislative competence of the devolved administration. The Minister must consult the Minister for the Cabinet Office, relevant Ministers from the other devolved administrations, Commissioners for HM Revenue and Customs, HM Treasury and other persons as the Minister considers appropriate. Devolved administrations may wish to work together to develop an objective

which applies across devolved territories. In such instances Ministers in the relevant devolved administrations will need to agree the drafting of the objective and make the regulations as appropriate.

32. Any proposal by a public authority within a devolved territory for the creation of a UK-wide objective should be discussed with the relevant Ministerial body in the devolved administration before it is formally proposed to the Minister for the Cabinet Office for consideration. Legislation only allows the Minister for the Cabinet Office to make regulations for the creation of UK-wide objectives under the power.

Purpose of the debt and fraud powers

33. It is estimated that losses to Government through fraud are in the region of £29bn to £40bn. It is in all our interests to prevent fraud, and public bodies have a particular responsibility to ensure that taxpayers' money is spent appropriately and is not taken out of the system fraudulently. The 2014 NAO report on Managing Debt Owed to Central Government estimated that around £22bn of debt was owed to Government in March 2013. At March 2016 it is estimated that the like for like debt balance rose to around £24.5bn.

34. Only debt owed to government that is legally collectable will be covered by these powers. Fairness is a key consideration in the exercise of the power to share data for the purposes of taking action in connection with debt owed to government. Any public authority(or private body fulfilling a public function on behalf of a public authority), who want to make use of this permissive power to share identified debt data to enable better debt management, including debt recovery, will need to consider fairness in their debt data sharing arrangements. The Fairness Principles are set out in Annex A.

35. The powers introduced by the Digital Economy Bill provide for the first time a simple and agile route for agreeing and establishing data shares between specified persons in order to protect them against fraud or to support them in the management of outstanding debt. These permissive powers are intended to ease the burden of establishing individual gateways or producing new legislation to ensure public authorities have the required legal powers each time or in each circumstance where they may wish to share data.

36. Steps have to be taken to ensure that data sharing proposals are balanced and proportionate and come under an appropriate level of scrutiny, similar to that which would be applied to the development of a gateway. Data sharing arrangements under these powers must comply with data protection legislation.

37. Parties wishing to share data under the fraud or debt power must put together a business case setting out the nature of the sharing required to fulfil their desired purposes, and must go through a pilot process to ensure that the sharing is effective.

38. Data sharing arrangements should be defined through a business case detailing the data sharing pilot to be undertaken. These data sharing pilot business cases will be scrutinised by a review group, which will include engagement with ICO, and recommendations made to a relevant Minister for approval. The process will be transparent, with all key information and privacy impact assessments made available to the general public for scrutiny

39. Information disclosed under the power can only be used for the purposes for which it was disclosed. There are very limited instances where information can be used by a public authority for another purpose. These circumstances include:

- If the information has already been lawfully placed into the public domain;
- If the data subject has consented to the information being used for the other purpose;
- For the purpose of a criminal investigation;
- For the purpose of legal proceedings; and
- For the purposes of safeguarding vulnerable adults or children, or protecting national security.

40. As with the public service delivery power, these provisions do not apply to personal information disclosed by HMRC, which includes the Valuation Office Agency (VOA). Personal information which is disclosed by HMRC cannot be used for a purposes other than the purpose for which it was disclosed unless with HMRC consent.

Which organisations can use the powers?

41. Chapters 1, 3 and 4 of Part 5 of the Digital Economy Bill provide permissive powers enabling specified public authorities or a person providing services to a specified public authority to disclose information for specific purposes. Bodies able to disclose information under the respective powers will be listed in regulations. Draft regulations can be found at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535311/2016-07-05_Digital_Government__Disclosure_of_Information__draft_regs.pdf

42. A public authority is defined for these purposes as a person or body who exercises functions of a public nature in the United Kingdom, a person or body entirely or substantially funded from public money, an office-holder appointed by a person or body falling within a body exercising functions of a public nature in

the United Kingdom, or a body more than half of whose governing body or members are appointed by a person or body exercising functions of a public nature in the United Kingdom.

43. The public service delivery, debt and fraud powers allow a person providing services to a public authority to share information. A person providing services to a public authority can be any legal entity such as a charity or company providing a defined service(s) to a public authority. This in effect could be a frontline service, which has been outsourced to a body outside the public sector to deliver. The key factor to consider is whether access to information held by such an organisation is critical to achieving the desired objective and similarly whether the delivery of better services could be improved by disclosing public sector information to them. An assessment must be made whether the persons providing services to a public authority have the systems and processes in place to securely handle data. The public authority receiving the services from the persons should make the assessment of the systems and processes the other party has in place, and should include details of the checks carried out within the privacy impact assessment.

44. A person providing services to a public authority sharing information under the powers can only disclose or use information for the functions/services it provides and for the specified purposes set out in the relevant provisions for its inclusion within the data sharing arrangement. For example, a data sharing arrangement relating to a Troubled Families programme may need to share information with a charity providing a service to a local authority within the region. The charity could only share information under these powers in relation to the service it provides to the local authority and not any other information it may hold, for example in respect of other services it provides in that region or other regions.

45. It is important that all public authorities and persons providing services to a public authority involved within a data sharing arrangement understand their roles and responsibilities in relation to information that they seek to use in the exercise of these powers, and are clear on what they may and may not access and share for these purposes. You must therefore adhere to and keep up to date with any guidance issued by the Information Commissioner in all instances where you are considering sharing information. This will ensure that consistent approaches and policies are being applied when considering requests to share information.

46. Prior to sharing information, you must first be satisfied that the sharing of information is in accordance with the purposes set out in legislation. You will need to strictly adhere to the DPA and ensure information is not disclosed where it is prohibited to do so under Part 1 of the Regulation of Investigatory Powers Act 2000.

Amending the list of bodies able to use the power

47. The public service delivery, debt and fraud powers will, by regulations, specify which public authorities can use the powers. The Minister for the Cabinet Office or relevant Minister from a Devolved Administration can make regulations to add, modify or remove a reference to a public authority or description of public authority allowed to share information under each of the powers.

48. If your public authority is not listed in regulations and you wish it to be in scope of the powers, your organisation will need to contact the relevant Minister with oversight for your work providing a case for its inclusion via regulations. The case should set out the systems and procedures in place for securely handling personal data as well as the reasons why they should be able to disclose and/or access data under the power. Where public authorities are based in England, the appropriate Minister, once satisfied with the case for inclusion should then write to the Minister for the Cabinet Office who will coordinate and lead the making of regulations. Devolved bodies should contact the relevant Minister in their devolved administration to make the necessary regulations.

Part 3: Data sharing and the law

How the powers work with other key legislation relating to data

49. To use the public service delivery, debt or fraud powers you will need to strictly adhere to the DPA and ensure no disclosures are made which are prohibited under section 1 of the Regulation of Investigatory Powers Act 2000. You will also need to ensure you are compliant with the Human Rights Act 1998. In addition, criminal sanctions for unlawful disclosure set out in section 19 of the Commissioners for Revenue and Customs Act 2005 will apply to personal information disclosed by HM Revenue and Customs.

Data Protection Act 1998

50. The DPA requires that personal data is processed fairly and lawfully and that individuals are aware of which organisations are sharing their personal data and what it is being used for. It should be noted that it is possible that some data disclosed under these powers will not constitute personal data, for example where data relating to deceased persons, businesses or information comprising only statistics that cannot identify anyone are being shared. Those making use of the powers, however, must be aware of their obligations under the DPA and must ensure that no disclosures are made under the power in contravention of those rules.

51. The Information Commissioner's data sharing code of practice recommends that where information is shared, it is shared in a way that is line with the reasonable expectations of the individual whose data it is. This approach applies to routine data sharing as well as to a single one-off data disclosure.

52. Public authorities will need to demonstrate that they are complying with the provisions contained in the DPA, and in particular must ensure they are handling personal data in accordance with the data protection principles, details of which can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/

Part 1 of the Regulation of Investigatory Powers Act 2000

53. The Regulation of Investigatory Powers Act 2000 provides a framework for lawful interception of communications, access to communications data, surveillance and the use of covert human intelligence sources. Part 1, Chapter 1 deals with interception. Section 1 of part 1 Chapter 1 makes it an offence, subject to exceptions, to intercept intentionally and without lawful authority any

communication in the course of its transmission by means of public postal service or public or private telecommunication system.

Human Rights Act 1998

54. Public authorities must ensure that data sharing is compliant with the Human Rights Act 1998 and in doing so must not act in a way that would be incompatible with rights under the European Convention on Human Rights.

55. Article 8 of the Convention, which gives everyone the right to respect for his private and family life, his home and his correspondence, is especially relevant to sharing personal information. Whilst sharing data relating to deceased individuals is not treated as personal data under the DPA as outlined above, Human Rights Act considerations should be taken into account with regards to whether sharing information could impinge on the rights to a private life for the relatives of deceased individuals.

56. The Information Commissioner's data sharing code of practice advises that if information is being shared in ways that comply with the DPA, it is also considered likely that the sharing would comply with the Human Rights Act.

Commissioners for Revenue and Customs Act 2005

57. HMRC's unlawful disclosure provision is governed by section 19 of the Commissioners for Revenue and Customs Act 2005, which makes wrongful disclosure of information relating to an identifiable person a criminal offence carrying a maximum penalty of imprisonment for up to 2 years and an unlimited fine. Section 19(1) makes it an offence for any person to contravene section 18(1), or of section 20(9), by disclosing "revenue and customs information relating to a person" whose identity is revealed by the disclosure. The term "person" includes both natural and legal persons, and, for example, the tax affairs of a limited company are also protected by section 19(1).

Part 4: Deciding to share information under the powers

58. The powers under Chapters 1, 3 and 4 of Part 5 of the Digital Economy Bill are permissive. Your public authority has the discretion to decide whether to use the power to disclose information and participate in a data sharing arrangement. You should consider which, if any, powers are already available to your organisation to achieve your desired policy, operational or analytical objective and determine whether these existing powers would adequately fulfil your objectives. This is to avoid the creation of unnecessary new express legal gateways where pre-existing powers already fulfil that function.

59. The main criterion for sharing information with specified recipients under these powers is that the sharing of information is consistent with and aligned to the purposes set out in primary legislation for each of the respective powers. You should place the same importance on the benefits that citizens can derive from better and more timely services as a result of information sharing as you do on protecting the privacy of citizens' data. This approach to sharing information is consistent with the National Data Guardian's 7th principle which relates to health and adult social care data in England that 'the duty to share information can be as important as the duty to protect patient confidentiality'.

60. You should factor the ethical considerations around the use of data to achieve the objective. The first iteration of the data science ethics framework is available at www.gov.uk/government/publications/data-science-ethical-framework and provides guidance on ethical considerations which are applicable to the sharing and use of data beyond data science. You should consider running a public consultation where you feel the general public may have concerns about the proposal. You should set out the details of the public consultation or the reasons for not carrying out one in the business case for the data sharing proposal.

61. When developing a data sharing proposal you should look to use the minimum amount of personal data possible. Consideration should be given to data matching which utilises binary checks against details of individuals to restrict the amount of personal information shared. The sharing of large data sets should only be considered where it would otherwise be inefficient or difficult to achieve the objective.

62. Before you establish a data sharing arrangement, you must be satisfied that:

- all parties are clear on the tangible benefits that are expected from the information sharing, who will receive them, how they will be

measured and where information about the data sharing arrangement will be made available online for public scrutiny;
- the purpose of the information sharing falls within the purposes outlined in legislation (or regulations for defined objectives for the public service delivery power);
- there is clear governance of, and accountability for, making the decision to share data;
- information sharing will be physically and/or technically possible and be compliant with the DPA and other relevant legislation;
- strict compliance with government and departmental security guidelines to safeguard against any misuse or loss of data, including having secure methods in place for transferring data;
- as the data controller, it is appropriate and sensible to take part in the arrangements - for example are there any perceived conflicts of interest with sharing information?; and
- The minimum required information will be disclosed, ideally to binary eligibility checks to mitigate against any risks around disclosure (for example risk of fraud or any other harm).

The Data Protection Principles and the powers to disclose data

63. Schedule 1 to the DPA sets out 8 Data Protection Principles governing the way personal data is to be collected, held and managed. These include the requirements that personal data should be processed lawfully and fairly, and for a specified purpose. Further, information should be shared securely, with appropriate protective measures in place (such as encryption and other methods). The disclosure of information under Chapters 1, 3 and 4 of Part 5 of the Digital Economy Bill may only be made for the purpose of enabling the recipient to fulfil objectives consistent with the purposes of the powers.

64. What constitutes fair processing will vary from case to case, but a key consideration will be the reasonable expectation of the individual whose data it is as to how their data would be handled or whether it would be disclosed. A further key indicator of fairness will be around transparency as to how the data is being processed.

65. You are required to ensure that your data sharing practices are fair and transparent and consider the effect the disclosure would have on the interests of the people whose data is involved. You will also be required to have fair and transparent processes in place for disclosing and receiving data. You must be satisfied that your processes are suitable for the types of data proposed to be disclosed before any data is shared. Before disclosing data you should discuss with the proposed recipients their arrangements for securely receiving, handling and managing the data and make an assessment of the suitability of the systems

and processes (which should be described in the data sharing agreement). In considering whether to share information, you must also consider whether conditions need to be imposed on the future use and retention of the data by way of data sharing agreements. Any conditions will need to be clearly specified prior to sharing information.

66. When sharing information under the powers you should look to operate as transparently as possible. Succinct and clear descriptions of why information is being shared, what information is being shared and the bodies with which they are being shared should be published online and easy for people to find alongside the relevant data sharing agreements, privacy impact assessments and other relevant documents. You should also provide and keep up to date contact details so that people know who to direct any concerns or queries to.

67. In some instances, such as where information is used to match data concerning a large number of individuals, it may be impracticable to send notices to individuals affected by the data sharing. You will however need to comply with requirements of the DPA in ensuring that data has been shared fairly and lawfully. It will also be necessary to make records of data shared, detailing the circumstances, what information was shared and an explanation as to why the disclosure took place. Business cases and data sharing agreements will be important documents in recording these decisions and the reasoning behind them.

68. In addition, the first data protection principle requires that organisations must be able to satisfy one or more "conditions for processing" in relation to their processing of personal data. The conditions for processing are set out in Schedules 2 and 3 to the DPA. Many (but not all) of these conditions relate to the purpose or purposes for which information is intended to be used, or the reason for the processing. Organisations processing data need to meet one or more of the conditions in either Schedule 2 or Schedule 2 and 3 depending on the data being shared. When sharing sensitive personal data the more exacting requirement to meet at least one condition in each schedule applies (and indeed the conditions are themselves more stringent). For a definition of what constitutes sensitive personal data see section 2 of the DPA. In some instances, you may consider additional data fields as sensitive in the context of a data sharing arrangement. In such circumstances you should discuss, agree and set out any restrictions or specific conditions for the processing of that data in the relevant data sharing agreement with other organisations involved.

69. Fulfilling a Schedule 2 (and where necessary, Schedule 3) condition will not, on its own, guarantee that the processing is fair and lawful – fairness and lawfulness must still be looked at separately. Part II of Schedule 1 of the DPA provides guidance on the interpretation of this principle. To assess whether or not personal data is processed fairly, you must consider more generally how it affects the interests of the people concerned – as a group and individually.

Best practice considerations

70. In addition to applying the principles of the DPA, you should consider what best practices and guidance are in place in your organisation and ensure you adhere to and keep up to date with them so that consistent approaches are being applied when sharing information. For the purposes of public service delivery power, it would be common practice to develop data sharing arrangements between organisations.

Fairness Principles for establishing pilots under the debt power

Fairness is a key consideration for the debt data sharing power in particular. If you wish to use the permissive power to share identified debt data to enable better debt management, including debt recovery, you will need to consider fairness in your debt data sharing pilot.

A set of fairness principles specifically for use with the debt powers can be found at Annex A. Your organisation will continue to have its own fairness policies and practice. These principles align with departmental practices, and aim to create a more consistent approach to fairness across the debt data sharing pilots. The Principles only apply to debt data sharing pilot activity to be carried out under this new power, and only in accordance with the legal obligations public authorities have a statutory duty to abide by.

The use of wider data sharing will help to enhance cross-government debt management capability, and help to enable a more informed view of a customer's individual circumstances and their ability to pay. Pilots under the data sharing power should aim to use relevant data to help differentiate between:

- A customer who cannot pay their debt because of vulnerability or hardship - so that individuals can, for example, be offered advice and guidance about the debt owed (where appropriate), or be signposted to non-fee paying debt advice and support, with the aim of minimising the build-up of further debt;
- A customer who is in a position to pay their debt - some of whom may need additional support; and
- A customer who has the means to pay their debt, but chooses not to pay - so public authorities, and private bodies acting on their behalf, can assess which interventions could best be used to recover the debt.

Non-public authority duties

71. Where a data sharing arrangement proposes that information be disclosed to a body which is not a public authority, but fulfils a public function, an assessment should be made of any conflicts of interest that the non-public authority may have and identify whether there are any unintended risks involved with disclosing data to the organisation. Non-public authorities can only participate in a data sharing arrangement once their sponsoring public authority has assessed their systems and procedures to be appropriate for secure handling data. Details will need to be set out in the privacy impact assessment along with a statement of compliance with the Code of Practice in the data sharing agreement.

Data standards and rights of redress

72. Public authorities hold vast amounts of data in a number of different formats. When considering sharing information it is essential that every effort is made to ensure that the format of the data conforms to any appropriate standards defined in the Government Standards Hub and the API standard. This will help ensure that individuals are not adversely impacted by any exchanges – e.g. prevented from accessing a service where there are issues with data held by a recipient as a consequence of the data exchange.

73. It is also important that checks are made on the accuracy of data prior to transferring it, in line with the DPA's Privacy Principles. In instances where issues arise following the transfer of data, procedures need to be in place to allow for inaccurate data to be corrected by all bodies holding the information. Organisations involved in a data sharing arrangement should agree procedures, the process of recording and capturing corrections for auditing purposes and contacting the data subject where appropriate and set the details out in the Data Sharing Agreement. You will need to be aware of the correct procedures to follow in relation to correcting inaccurate data held on your own systems, including alerting officials responsible for data protection within your organisation and other identified teams to ensure data is corrected where held on other systems.

Checklist - points to consider
Why share

- For what purpose and public function is the information being requested?
- Are there any other benefits of the data exchange for the receiving party or any other public body?
- What are the implications of not sharing information? – e.g.
    - Increased risk that people do not receive the support or the

services they require in a timely manner;
  - Risk that burdens will be placed on people to repeatedly supply information to access the services they require; and
  - Risk of wasting taxpayers' money by jeopardising public finances or commercial projects.

What to share

- What exact data items are required and why?
- Are there any express legal restrictions in place on the disclosure and use of the data involved and are there any legal obligations on the recipient of the data to provide it to any other bodies?
- How regularly and in what volume is it proposed to share the data?
- Are there any ethical issues with the proposed data sharing arrangement?

How to share

- What methods or technology can be used to minimise the amount of information shared and risk of data loss e.g. using aggregate data, derived data or the use of a look-up process, in preference to bulk data sharing
- What procedures will be in place to correct any inaccurate data identified during the data sharing process and the process for capturing the changes made for auditing purposes?
- What are the conditions for processing information, will data subjects be aware that their data is being processed and will procedures for dealing with access requests, queries and complaints be in place?
- Information handling responsibilities, including details of any data processors, contractors or subcontractors;
- Security considerations, e.g. the use of secure transfer mechanism, and encryption;
- For audit purposes document the process and methods of exchange, how exchanges are logged, what information is stored and who has access to it;
- Standards and levels of expected operational service;
- Termination arrangements;
- Minimising cost of providing/transferring the data;
- Issues, disputes and resolution procedures;
- Sanctions for failure to comply with the agreement or breaches by individual staff;
- Is there a time-limit suggested for using the data and if so how will the data be deleted?; and
- Periodic reviews of effectiveness and necessity of data sharing arrangement.

Part 5 - Fairness and transparency

74. You are required to ensure that your data sharing practices are fair and transparent. You should only share data once you are satisfied that the processes are fair and transparent. Under the debt and fraud powers, the secretariat to the Review Group will centrally maintain and make available online a list of pilots under the power, setting out the title, reason and potential benefits to be gained from the data sharing arrangement.

75. All organisations wishing to establish a data sharing arrangement under the power must adhere to the Information Commissioner's data sharing code of practice on Data Sharing. The process of establishing a data sharing arrangement under the public service delivery, fraud and debt powers vary in the following ways:

- The fraud and debt powers require a formal application process to allow the strategic management of data sharing arrangements under the powers during its three year review period;
- The public service delivery power operates as a more conventional legal gateway permitting specified persons to share information for defined purposes.

76. If you are looking to share information under any of the three powers you need to carefully consider why a data sharing arrangement should be established and maintain an audit trail of decisions to ensure that informed decisions on data sharing are made by public authorities at the right level in the organisation. Conducting a privacy impact assessment of the proposal should be one of the first steps you take. It will help you assess the potential benefits against the risk or potential negative effects, such as an en erosion of personal privacy.

77. The public service delivery, debt and fraud powers require a number of documents to be produced. These documents are:

- A business case for the data sharing arrangement (this can be co-developed by all the organisations involved);
- data sharing agreement(s); and
- security plan

78. You should operate as transparently as possible. Business cases, data sharing agreements and privacy impact assessments should be made available to the general public. You may wish to redact some sensitive information from your business case to establish a fraud pilot if you feel placing that information in the public domain could undermine achieving the objective of the data sharing arrangement. You should include a high level summary of the security plan in the

business case and avoid publishing the full security plan to reduce the risk of hacking.

Business Cases

79. If you wish to establish a data sharing arrangement under the public service delivery, debt and fraud powers you must develop and agree a business case with the other bodies participating in the data share. A single business case will need to be developed for each data sharing arrangement. A data sharing arrangement can cover multiple transactions. Your business case must contain:

- the objective of the data sharing arrangement;
- a list of which bodies will be involved in the arrangement, and specifically which bodies would disclose or receive data, what type of data is involved, and what restrictions are in place on the data;
- an explanation of how the data will be used and what the conditions for processing are;
- the information sharing agreements that will be used in practice;
- fair processing notices that are relevant and appropriate;
- an explanation of how retention periods will be complied with and how they will continue to meet business needs;
- an assessment of the ethical considerations on the proposed data sharing arrangement;
- a statement of adherence to this code of practice;
- an outline of what the activities, delivery plan, costs and potential benefits are;
- an explanation of what steps will be taken to address any data quality issues identified;
- an outline of the data security arrangements to be put in place and the checks that will be run to ensure that all bodies involved are compliant (a separate security plan will need to be produced but public authorities may not wish to make this document available to the general public); and
- an outline of the accountability process for the data sharing arrangement including senior responsible owners and record of data sharing that has taken place for audit purposes.

80. As data sharing under the debt and fraud powers must be piloted, your business case for a pilot must also contain:

- high level details of the effective anti-fraud measure, or debt management measure;
- a period of duration;
- a statement of success criteria; and
- details of the methodology for measuring success.

81. Business cases provided under the fraud power need not go as far as detailing the counter fraud operation of partners. The intention of the business case is to justify the pilot and ensure that data is being protected.

Privacy Impact Assessments

82. A privacy impact assessment is a process which helps identify and reduce the privacy risks of a data share. You must conduct a privacy impact assessment if you wish to share data under the public service delivery, debt and fraud powers. The ICO's Conducting Privacy Impact Assessments code of practice[1] provides guidance on a range of issues in respect of these assessments, including the benefits of conducting privacy impact assessments and practical guidance on the process required to carry one out. The privacy impact assessment should be reviewed at critical milestones and updated where necessary (for example when a pilot under the debt or fraud power has demonstrated benefit and is to be upscaled).

83. A privacy notice describes all the privacy information you make available or provide to individuals about what you do with their personal information. In exercising these powers to share data, you must ensure that suitably worded privacy notices are published and made available to the public in line with fairness and transparency principles in the Information Commissioner's privacy notices code of practice[2] and data sharing code of practice. The Information Commissioner's privacy notices code of practice provides guidance on the content of these notices, as well as where and when to make them publicly available.

Data Sharing Agreements

84. You should follow the Information Commissioner's data sharing code of practice with regards to data sharing agreements. Before entering into data sharing agreements, you will need to agree with the other organisations involved in the data share that they will take appropriate organisational, security and technical measures to:

- ensure information will be retained securely and deleted once it has been used for the purpose for which it was provided;
- prevent accidental loss, destruction or damage of information; and
- ensure only people with a genuine business need have access to the information.

85. The data sharing agreements will not be legally binding. You will be expected to include details of:

a. the purpose of the data sharing arrangement;
b. the respective roles, responsibilities and liabilities of each party involved in the data share;

c. the legal basis for exchanging information;
d. the accuracy of the data – ensuring that the recipient is aware that data is only as accurate as at the time it is captured and will be treated as such;
e. precise details of what exact data is required to enable them to perform the function for which it is requested;
f. restrictions on sharing certain categories of data;
g. restrictions on any onward disclosure of information - if applicable;
h. information handling responsibilities, including details of any data processors or subcontractors;
i. conditions for data processing, including whether data subjects are aware of how their data is being shared, including the methods of sharing and whether they are likely to object to it;
j. process and methods of exchange;
k. standards and levels of expected operational service;
l. reporting arrangements, including any reporting in the event of any data loss and handling arrangements;
m. termination arrangements;
n. issues, disputes and resolution procedures;
o. information on data security, data retention and data deletion;
p. review periods;
q. individuals' rights – procedures for dealing with access requests, queries and complaints;
r. any costs associated with sharing data; and
s. sanctions for failure to comply with the agreement or breaches by individual staff.

86. The above list is not exhaustive. For more detail on data sharing agreements you should refer to the ICO data sharing code of practice.

87. Data sharing agreements should contain details of sanctions that will apply to recipients of information who are found to be unlawfully or inappropriately processing data. These sanctions will include, but are not limited to:

- Public authorities ceasing to receive information from other public authorities under the relevant power in the Digital Economy Bill. Regulations may be made to remove the organisation from the list of bodies able to share information under the power;
- Public authorities considering whether a given incident and/or organisation needs to be reported to the Information Commissioner's Office;
- Public authority officials determining whether any misuse of public office offences have been committed, and if so, to take any necessary action; and
- Persons granted access to information following a previous data breach will be required to have their systems and procedures assessed by a sponsoring public authority. Such persons will only be able to participate in a data

sharing arrangement once public authority officials are satisfied that any security or other issues have been resolved to reduce the risk of any further issues occurring again in the future. The data sharing agreement should capture details of the assessments and the steps that have been taken to address previous problems.

88. A register of data sharing arrangements under the debt and fraud powers will be maintained centrally and by the secretariat to the Review Group in the Cabinet Office for audit purposes. The Review Group is an oversight panel which will be constructed of representatives from across the government and privacy interest groups. It will include representation from the ICO. Its role is to check that data sharing arrangements adhere to this code of practice and that the arrangement can operate under the legislation. All public authorities sharing information under the public service delivery, fraud and debt powers are required to maintain records of their individual data sharing arrangements for audit purposes.

89. You will need to comply with the DPA and where necessary seek legal advice regarding data sharing following any agreements to disclose or access information.

The process for establishing data sharing arrangements under the debt and fraud powers

90. All data sharing proposals under the debt and fraud powers must be piloted to determine whether there is value in sharing personal information for the purposes set out in the relevant parts of the bill, namely to take action in connection with debt owed to government, or to combat fraud against the public sector.

91. Strong central governance is required to oversee the running of pilots to ensure there is consistent and appropriate use of the powers. A Review Group will be established by the UK Government to oversee any UK-wide and England only data sharing under the debt and fraud powers. The review group will also be responsible for collating the evidence which will inform the Minister's review of the operation of these powers, as required under the Bill after three years. This evidence will be gathered from the UK-wide and England only data sharing arrangements as well as those implemented in the devolved territories. The devolved administrations will establish their own governance structure for oversight of data sharing arrangement within their respective devolved territories. Data pertaining to the operation of pilots in the devolved territories should be periodically submitted to the secretariat for the Review Group for the purpose of collating the evidence for the review of the debt and fraud power after three years.

92. The Review Group and secretariat will be established to take responsibility for the strategic management of pilots established under the power to ensure bodies carrying out pilot data shares under these provisions operate with regard to the Code, and to gather and analyse evidence on the effectiveness of pilots to enable the review of the power after three years. The Review Group will also consider complaints and take account of the views of the Information Commissioner's Office. All proposals for pilots must be submitted to the Review Group through the secretariat. It is envisaged that the Review Group will sit monthly and that requests and clearance through the Minister should take around 6 weeks once an application has been submitted.

93. The Review Group will consist of appropriately qualified subject matters experts gathered from across government and will be attended by representatives from the ICO and members from public representative bodies. The secretariat will keep a record of pilots in operation and how those work, and will gather from the bodies operating the pilot the appropriate performance data for the recording and evaluation of the pilot.

94. If you wish to establish a pilot you must submit a business case to the secretariat to the Review Group. A single business case will need to be submitted which is agreed by all the participating bodies.

95. On receipt of a given business case, the secretariat will confirm with you whether it is suitable for submission to the Review Group and will let you know the date by which the business case will be considered by the Review Group.

96. The Review Group will review the business case and advise you whether the proposal meets the requirement to use the power, and whether the request should be declined, amended or be recommended to the Minister for the Cabinet Office to be implemented.

97. Business cases may be declined for a range of reasons, for example the proposal may require modification to align it to best practice, or to more clearly define success criteria and methodology for measuring them, or the recommendation that alternative routes may be more appropriate. Pilots will become active upon confirmation from the Minister that the recommendation has been approved.

98. During the operation of the pilot, you are responsible for:

- adherence to the terms of the pilot;
- reporting on the performance of the pilot;
- reporting of any variation in the pilot, either as a request to Review Group, or as a deviation and breach of the code; and
- closure of the pilot and final reporting.

Data Security

99. All persons and bodies involved in any data sharing arrangements under these powers will be subject to the data protection principles set out in the DPA.

100. Additional requirements include:

- Public authorities and receiving parties must satisfy themselves that all departmental or local authority standards and protocols are followed when providing or receiving information.
- Each party involved in the data share must ensure effective measures are in place to manage potential or actual incidents relating to the potential loss of information.
- In the event of a potential or actual data incident, public authorities and data processors, together with any other additional third parties must be fully engaged in the resolution of the data incident. The responsibilities of each party in the event of a potential or actual loss of information must be clearly defined in the data sharing agreement and or security plan.

101. You will need to agree a security plan as part of any formal data sharing agreements with public authorities who are granted access to information. Security plans should include:

- storage arrangements that ensure information is secured in a robust, proportional and rigorously tested manner;
- assurance that only people who have a genuine business need to see personal information involved in a data sharing arrangement will have access to it;
- confirmation as to who to notify in the event of any security breaches; and
- procedures in place to investigate the causes of any security breaches.

Data retention and disposal

102. It is a requirement of the DPA that personal information should be kept only for as long as necessary. How long it is “necessary” to hold such information will depend on the purpose for which the public authority holds the information, and its own policies and practices.

103. You will need to agree with recipients of data shared under these powers how long the data is expected to be held for and the period agreed should be documented in any data sharing agreements between both parties.

104. You should ensure that data no longer required is destroyed promptly and rendered irrecoverable. The same will apply to data derived or produced from the

original data, except where section 33 of the DPA applies (in relation to data processed for research purposes). You should refer to the ICO guidance on Deleting Personal Data[3].

[3] https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf

Part 6: Governance

Implementing a data sharing arrangement

105. Data sharing under the power must adhere to the Information Commissioner's data sharing code of practice and other existing guidelines on data security. You must respond swiftly and effectively to any complaints, objections or requests under the right of access to personal information. You should periodically run checks to ensure data security best practice is adhered to and publish details online of what checks were carried out and when.

106. Where data quality issues are identified during a data sharing arrangement, the governance structure supporting the data sharing arrangement should take immediate steps to identify and manage the risks associated with the use of that data and any remedial action required.

107. The ICO has a general power to conduct audits (including compulsory audits of government departments, designated public authorities and other categories of designated persons) of organisations to check that they are complying with law in relation to the handling of personal information. All bodies are required to comply with the ICO's request for assistance so that they can determine whether data has been processed lawfully within the data sharing arrangement. The ICO is able to take criminal proceedings where necessary and will report any concerns about a body's systems and procedures for handling data to the relevant Minister (MCO for England only and UK-wide data sharing initiatives and the relevant Minister in the devolved administration for a data sharing arrangement within a devolved territory only), which may result in regulations being laid to exclude that body from participating in a data share under the power.

108. You should make it easy for citizens to access data sharing arrangements and provide information so that the general public can understand what information is being shared and for what purposes. You should communicate key findings or the benefits to citizens derived from data sharing arrangements to the general public to support a better public dialogue on the use of public data.

Review of a pilot under the debt and fraud powers

109. A Review Group will be established by the UK Government to oversee any UK-wide and England only data sharing under the debt and fraud powers. The review group will also be responsible for collating the evidence which will inform the Minister's review of the operation of these powers, as required under the Bill after three years. The devolved administrations will establish their own

governance structure for oversight of data sharing arrangement within their respective devolved territories.

110. A request to initiate a pilot to be carried out under the debt and fraud powers must be sent to the appropriate review group for your territory accompanied by a business case. Your business case must detail: its operational period, the nature of the fraud or the debt recovery issue being addressed, the purpose of the data share and the way its effectiveness will be measured.

111. At the end of the pilot's operational period its outcome will be presented to the review group for consideration, with an accompanying: proposal, actions or recommendation. For pilots designed to test a proposed data share under these powers, successful execution of the pilot may result in agreement that the process can at that point run as a 'business as usual' process (i.e. an ongoing data sharing arrangement) without any requirement for further reporting or management.

112. If the pilot has proved to be unsuccessful in meeting the defined requirements, then the pilot must be stopped. Any design changes that have been recognised during its operation that would make it successful should be submitted as a request for a new pilot.

Compliance with the Code

113. Any serious security breaches need to be reported immediately to the ICO, the Review Group and where applicable, the governance group in your devolved territory.

114. You should also report immediately any breaches regarding adherence to the code or any sharing that contravenes the terms of the data sharing arrangement but does not constitute a DPA breach. Such breaches to the code or data sharing arrangement relating to data sharing under the public service delivery power should be reported to the relevant person within the governance structure as relevant to the particular data sharing arrangement, whilst breaches under the debt and fraud powers should be reported to the review group for your territory.

115. Under the debt and fraud powers, the review group will inform the relevant public authorities that a breach has been reported, and will investigate the breach. In doing so, it may make one of the following findings:

- There is deemed to be no breach and no action is required.
- A breach is found to have taken place but deemed to be of low impact: it will notify the public authority and ask it to introduce measures to remedy this.

- A breach is found to have taken place but is deemed to be of such seriousness that the pilot must be stopped: in this case, it will notify the public authority of the finding and inform the Minister of its recommendation.
- A breach is found but deemed to be so serious that the public body must be removed from the schedule. In such cases, it will notify the public authority of the finding and inform the Minister of its recommendation.

116. Where the Minister has been informed by the Review Group under the debt and fraud powers of a recommended course of action regarding a breach, the Minister will notify the public authority and the Review Group as to the course of action he wishes to pursue. The Minister may in addition notify the ICO. There will be a right to appeal at each stage.

117. You should address any general questions and concerns about the debt and fraud powers to the Secretariat in the first instance.

Review of the debt and fraud powers

118. You are required to report on the progress of your pilot (including the success or failings) to the relevant Review Group for your territory. These reports will support the overall evaluation of the operation of the powers, and will be used to inform the Minister's review at the end of the three-year period, as required under the provisions. This evidence will inform the Minister's assessment of the provisions and will enable him to prepare his report setting out the findings of his review.

Annex A - The Fairness Principles for data sharing under the debt power

Fairness is a key consideration in respect of the operation of the debt data sharing power. Public authorities will continue to have their own fairness policies and practice. These Principles aim to align with existing public authority practices, and aim to encourage a more consistent approach to fairness across the debt data sharing pilots. The Principles only apply to debt data sharing pilot activity to be carried out under this new power, and only in accordance with the legal obligations public authorities have a statutory duty to abide by.

Pilots operating under the new data sharing power should aim to use relevant data to help differentiate between:

- A customer who cannot pay their debt because of vulnerability or hardship - so that individuals can, for example, be offered advice and guidance about the debt owed (where appropriate), or be signposted to non-fee paying debt advice and support, with the aim of minimising the build-up of further debt;
- A customer who is in a position to pay their debt - some of whom may need additional support; and
- A customer who has the means to pay their debt, but chooses not to pay - so public authorities, and private bodies acting on their behalf, can assess which interventions could best be used to recover the debt.

The use of wider data sharing for this purpose will help enhance cross-government debt management capability, and will help to enable a more informed view of a customer's individual circumstances and their ability to pay.

Pilots must be conscious of the impact debt collection practices have on vulnerable customers and customers in hardship. Statistical and anecdotal evidence from debt advice agencies shows that in a substantial amount of cases, a customer who has an outstanding debt will owe money to more than one creditor. The aim is to ensure any repayment plans are affordable and sustainable. This should balance the need to maximise collections, while taking affordability into account. This may be achieved by:

- Using relevant sources of data and information to make informed decisions about a customer's individual circumstances and their ability to pay. This process could include:
    - An assessment of income versus expenditure to create a tailored and affordable repayment plan based on in work and out of work

    - considerations, including the ability to take irregular income into account; and
    - Consideration of the need for breathing space to seek advice, or forbearance, in cases of vulnerability and hardship.
- Where a vulnerable customer is identified, they should be given appropriate support and advice, which may include signposting to non-fee paying debt advice agencies.
- Government should liaise with non-fee paying debt advice agencies who are helping customers in debt.
- Communication should clearly set out relevant information to enable the customer to take action, and encourage them to engage with the Government.
- Any pilot that uses a third party (such as a Debt Collection Agency or Shared Services) must also treat people fairly, in line with these Principles and relevant regulatory rules.
- Pilots should undertake regular engagement with stakeholders to encourage regular feedback about how fairly the pilots are working in practice.

Annex B - Summary of the process for using the public service delivery power

Step 1 - Identify the policy objective and the data needed to support it

- Do you need to use personal information?
    - Familiarise yourself with the DPA and the Information Commissioner's data sharing code of practice on information sharing
- Does the proposal pose any ethical issue or will it lead to any handling risks?
    - Refer to the Data Science Ethical Framework
    - Consider running a public consultation
- How do you want to share data and will it be secure?
    - Assess the data you need and ensure you can justify why you need each data field
    - Speak to your organisation's information governance and security experts and discuss what the best methods for data transfer are available.

Step 2 - Develop the proposal

- Agree a proposal with the other organisations involved in the data sharing arrangement
    - If bodies outside the public sector are involved you should consider any conflicts of interest and reflect it in the business case
    - Ensure all bodies are willing to comply with this Code of Practice
    - Seek advice from your legal advisers that your proposal is suitable for use under the public service delivery power and is consistent with the DPA and Part 1 of RIPA
- Conduct a privacy impact assessment

    - Assess the potential benefits of the data sharing arrangement against the risks or potential negative effects, such as an erosion of personal privacy
- Develop and draft a Business Case, data sharing agreements, a privacy impact assessment and Security Plan.
    - Ensure you refer to ICO guidance on data sharing agreements and privacy impact assessments
    - Ensure the responsibilities for each body involved in the data sharing arrangement is made clear and articulated in the documentation
    - The outcomes of any public consultation or, if a decision was taken not to undertake public consultation, the reasons for that decision, should be articulated in the business case
    - Ensure each organisation involved in the data sharing arrangement has the appropriate systems and procedures in place to handle data securely and that a security plan has been agreed which sets out how data security will be managed.

Step 3 - Operating the data sharing arrangement

- Managing the data sharing arrangement
    - You should ensure you apply fairness and transparency principles as set out in the ICO Code of Practice on Data Sharing
    - You should ensure the business case, data sharing agreement and privacy impact assessment are made available to the public and are easy for the general public to find
    - You should ensure that all bodies adhere to the data sharing agreement and security plan and report any data breaches as appropriate
- Assessment of the data sharing arrangement
    - At the conclusion of a data sharing arrangement you should assess and review that arrangement and consider communicating to the general public the findings including any benefits derived. This will help improve understanding of data sharing and also help share best practice and lessons learned with other public authorities. Finally, you should ensure that arrangements for the destruction of data have been fully implemented.

Annex C - Summary of the process for using the fraud and debt powers

Step 1 - Identify the policy objective and the data needed to support it

- Do you need to use personal information?
    - Familiarise yourself with the DPA and the ICO Code of Practice on information sharing
- Does the proposal pose any ethical issue or will it lead to any handling risks?
    - Refer to the Data Science Ethical Framework
    - Consider running a public consultation
- Can the data share be piloted and what would the method for measuring success/failure?
    - Contact the relevant central review group for your national territory for advice
    - Discuss with your analysts what would be suitable measures to evaluate the particular data sharing arrangement
- How do you want to share data and will it be secure?
    - Assess the data you need to share and ensure you can justify why you need each data field
    - Speak to your organisation's information governance and security experts and discuss what the best available methods are for data transfer.

Step 2 - Develop the proposal

- Agree a proposal with the other organisations involved in the data pilot
    - If bodies outside the public sector are involved you should consider any conflicts of interest and reflect this in the business case
    - Ensure all bodies are willing to comply with this Code of Practice
    - Agree success/failure criteria for the pilot
    - Seek advice from your legal advisers that your proposal is suitable for use under the relevant power (fraud or debt) and is consistent with the DPA and Part 1 of RIPA

    - If your proposal relates to debt, consider how the fairness principles can be embedded into the proposal
- Conduct a privacy impact assessment
    - Assess the potential benefits against the risks or potential negative effects, such as an erosion of personal privacy
- Develop and draft a Business Case, data sharing agreements, a privacy impact assessment and security plan.
    - Ensure you refer to ICO guidance on Data Sharing Agreements and privacy impact assessments
    - Ensure the responsibilities of each body involved in the data sharing arrangement are made clear and articulated in the documentation
    - The outcomes of any public consultation or decision as to why a public consultation did not take place should be articulated in the business case
    - Ensure each organisation involved in the data sharing arrangement has the appropriate systems and procedures in place to handle data securely and that a security plan has been agreed which sets out how data security will be managed.

Step 3 - Submitting the proposal

- Submit your proposal to the relevant central review group for your territory
    - Contact your central review group [D.N. details to be provided] and submit the relevant documentation to them
    - You may receive an initial view from the central review group with any recommendations they may have for strengthening the proposal, which you should respond to accordingly to enable the proposal to progress
    - The central review group will contact you to let you know whether a) your proposal will be recommended to the relevant Minister; b) whether modifications are recommended; or c) the proposal has not met requirements and an alternative approach should be pursued.
    - Your central review group will contact you to let you know whether the Minister is content for the pilot to proceed and the updates that will be required so that they can monitor progress

Step 4 - Running the pilot

- Managing the pilot

    - Upon receiving confirmation that the pilot may proceed, you should ensure there is an appropriate governance structure in place for the pilot
    - You should ensure that all bodies taking part in the relevant arrangement adhere to the data sharing agreement and report any breaches as appropriate to the central review group for your territory. Serious data security breaches should be reported to your central review group and the ICO
- Reporting to the central review group in England
    - Send appropriate metrics data about your pilot through at agreed intervals to the secretariat to the Review Group
    - The secretariat will publish relevant information about the pilot online and update with metrics as appropriate
    - At the end of the pilot period send a summary of the findings, and other relevant information to the Review Group
- Assessment of the Pilot
    - The central review group for your territory will analyse the metrics and findings of the pilot and make a recommendation to the relevant Minister as to whether it has met its objectives and whether the data sharing should proceed or not. The review group will contact you to inform you of the Minister's decision.
    - If the decision is to stop the pilot, you must ensure that steps are taken to destroy any copies of data acquired under the power.

Home Office

Data Sharing Code of Practice

Code of Practice for civil registration officials disclosing information under section 19AA of the Registration Service Act 1953 (as amended by the Digital Economy Act [2017])

Date: 19 October 2016

Civil Registration: Data Sharing Code of Practice

Produced by the Home Office

Contents

Part 1: About the Code of Practice

1. This Code explains how the discretionary powers contained in the Registration Service Act 1953 (as amended by the Digital Economy Act [2017]) should be used for the sharing of registration information[1] held by registration officials[2] with specified public authorities for the purpose of the public authorities fulfilling their functions. In addition, it provides details of the procedures that need to be followed when considering requests to use registration information including details about application processes, decision-making processes and governance procedures.

2. This Code should be read alongside the Information Commissioner's data sharing code of practice which provides guidance on how to ensure personal data is shared in a way that is lawful, proportionate and compatible with the Data Protection Act 1998 (DPA) and other relevant legislation such as the Human Rights Act 1998. The Code should also be read in conjunction with procedural guidance that registration officials already follow when sharing information. This will ensure that responsibilities for sharing information are defined, controlled and managed at the right level.

3. The Code defines 'data sharing' in the same terms as the Information Commissioner's data sharing code of practice[3], namely the disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. The ICO Code states that data sharing can take different forms including:

    - a reciprocal exchange of data;

[1] Registration information relates to any information held by a registration official in the exercise of his or her registration functions – e.g. information held relating to births, adoptions, stillbirths, marriages, civil partnerships, gender and deaths.

[2] A "registration official" is any of the following:
(a) The Registrar General;
(b) A Superintendent Registrar;
(c) A Registrar;
(d) A registration authority or a person exercising the functions of a registration authority;
(e) A civil partnership registrar (within the meaning of Chapter 1 of Part 2 of the Civil Partnership Act 2004 – see section 29 of that Act).

[3] https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

- one or more organisations providing data to a third party or parties; and
- several organisations pooling information and making it available to each other.

4. When making disclosures under the data sharing powers, data sharing agreements will be put in place to outline the responsibilities of recipients of data and any necessary actions that need to be taken should any issues emerge. The Code provides details of actions that may be taken to address any issues associated with either unlawful data disclosures or other disclosures that are outside of any formal data sharing agreements between registration officials and recipients of data.

5. Public authorities will need to satisfy themselves that they are complying with the Data Protection Act and will be advised to seek their own legal advice regarding data sharing, including any onward sharing following any agreements to access registration information. There are also instances where conditions form part of data sharing agreements including arrangements relating to how data is to be used by the recipient – see section on Data Sharing Agreements.

6. The Information Commissioner's Office has been consulted in the preparation of the Code to ensure that it aligns appropriately with the Data Protection Act and its own data sharing Code of Practice.

The Code's status

7. The Registrar General has prepared and published this Code under section 19AA of the Registration Service Act 1953 (as amended by the Digital Economy Act [2017]). It is a statutory Code which has been approved by the Minister for Immigration and laid before Parliament.

8. The Code does not impose additional legal obligations, nor is it an authoritative statement of the law. Registration officials must however have regard to the Code when sharing information with public authorities and follow the procedures outlined in the Code.

Specific benefits in using the Code

9. The key benefits of using the Code include:

- **Compliance with current policies and guidance**
  The Code will help ensure that registration officials are following the most appropriate policies and guidance when sharing registration information. By complying with guidance, registration officials can be confident that they are sharing information in a way that is consistent, fair, proportionate and transparent.

- **Compliance with legislation**
  The Code provides guidance on procedures to be followed to help ensure that registration officials are complying with the law when sharing information. These include adherence to the Data Protection Act 1998 and the Human Rights Act 1998.

- **Security Provisions**
  The Code outlines how information is held and controlled by registration officials. This includes details of the safeguards that are in place for protecting information and measures to prevent information being shared where there is no legal or justifiable basis for sharing information. In addition, it includes policies around data retention, destruction and provisions that ensure that data is not retained for longer than is required.

- **Competency and awareness**
  The Code highlights the importance of keeping staff updated and appropriately trained in data management, and aware of the criteria that has to be followed when considering granting access to information.

Part 2: Understanding the civil registration powers

The gateway in the Registration Services Act (as amended)

10. Section 19AA of the Act provides authority for registration officials
    - To disclose information held in connection with any of their functions.
    - With:
        - A specified public authority (as defined by section x of the Act); or
        - Any other civil registration official.
    - If they are satisfied that the public authority or civil registration official to whom it is disclosed requires the information to enable them to exercise one or more of their functions.

11. A civil registration official is defined as:
    - the Registrar General
    - a superintendent registrar of births, deaths and marriages
    - a registrar of births, deaths or marriages
    - a registration authority, as defined by section 28 of Civil Partnership Act 2004

Restrictions on this type of disclosure

12. The provisions do not allow for disclosure where there are current express statutory restrictions on sharing information. Where there are restrictions on the sharing of particular data relating to adoptions[4], or gender recognition[5], for example, those will continue to apply and the personal data may only be disclosed subject to those restrictions.
    [An Annex will be included containing two areas of further information to assist the reader of the code:

[4] See section 79(3) and 81(3) Adoption and Children Act 2002.

[5] See section 22 Gender Recognition Act 2004, although presumably sharing protected information under this new power would not be an offence by virtue of section 22(4)(j). Paragraph 3(4) of Schedule 3 to the 2004 Act provides that certain information is 'not to be open to public inspection or search' but this does not seem to prohibit disclosure to specified public bodies. The same provision (about public inspection or search) is made in regulations 5(3) and 15(3) of SI 2015/50 (concerning the Gender Recognition (Marriage and Civil Partnership) Registers)

Civil Registration: Data Sharing Code of Practice

1. A list of the statutory restrictions on sharing registration information. This document will set out clearly the types of data where there are such restrictions.

2. It will also provide examples of registration data that would be sensitive personal data to assist the reader but that list will not be exhaustive.

Part 3: Data sharing and the law

Data Protection Legislation

13. Disclosure under the Registration Service Act 1953 must also comply with the Data Protection Act and the Human Rights Act 1998.

14. This Code will assist you to determine whether a particular disclosure is in line with the above mentioned legislation and government policy on data sharing.

15. It will also assist in determining whether a formal data sharing agreement is required and what needs to be included in the agreement.

The Data Protection Act 1998

16. The Data Protection Act requires that personal data be processed fairly and lawfully and that data subjects are able to establish which organisations are sharing their personal data and what it is being used for. Some data sharing however does not involve personal data, for example data relating to deceased persons or where only statistics that cannot identify anyone are being shared. The Data Protection Act therefore does not apply in these instances, but disclosure will still need to comply with the Human Rights Act.

17. Registration officials will need to demonstrate that they are complying with the provisions contained in the Data Protection Act including adhering to data protection principles.

Data Protection Principles

18. The Data Protection Act sets out 8 basic principles which must be applied to the way personal data is collected, held and managed. These are:

I. Processed fairly and lawfully. There must be a lawful basis for obtaining, holding and sharing the data and the data must only be processed in a way that the individual would reasonably expect.

II. Obtained for specified and lawful purposes. Data must only be obtained for specified purposes and can only be disclosed if the disclosure is compatible with those purposes.

III. Adequate, relevant and not excessive. Only information that continues to be relevant should be kept. When making disclosure only information relevant and necessary for the purpose for which it is being disclosed should be shared.

IV. Accurate and up to date. Information should be accurate and up to date. (In relation to civil registration, records are required to reflect the facts at the time of the event and may only be corrected where an error has occurred via the processes set out in law).

V. Not kept any longer than necessary. Information should only be kept for as long as necessary and deleted once it is no longer required for the purposes for which it was collected. (Civil registration data is kept by registration officials forever, as is required by law, whilst other records such as details of certificate applicants, would be subject to office retention/disposal policy). A public authority collecting civil registration data must adhere to this principle though.

VI. Processed in accordance with the individual's rights. Individuals have the right to have factually incorrect information corrected. In addition, this principle also allows individuals to have access to personal information held about them – e.g. Subject Access Requests.

VII. Securely kept. Organisations holding personal information are required to have adequate security measures in place to ensure appropriate processing of personal data and to ensure personal data is not lost or stolen.

VIII. Not transferred to any other country without adequate protection in place. Personal information must not be sent outside

the European Economic Area unless the data subject has consented or adequate protection in the receiving country is in place.

19. For more detail on these 8 principles see https://ico.org.uk/for-organisations/guide-to-data-protection/ or contact your local data protection adviser.

20. The Information Commissioner's Office has also produced the following statutory data sharing Code of Practice, which on page 9/10 refers to working definitions of systematic (routine) and exceptional (ad-hoc) forms of sharing data. The guidance contained in the Code is particularly useful in determining how different approaches apply to these two types of data sharing. Registration officials, in collaborating with public authorities and other registration officials requesting data, will be able to identify whether the request is systematic or exceptional and will be able to determine the appropriate courses of action required in accordance with the data requested.
https://ico.org.uk/media/1068/data_sharing_code_of_practice.pdf

Human Rights Act 1998

21. Registration Officials must ensure that data sharing is compliant with the Human Rights Act 1998 and in doing so must not act in a way that would be incompatible with rights under the European Convention on Human Rights.

22. Article 8 of the Convention, which gives everyone the right to respect for his private and family life, his home and his correspondence, is especially relevant to sharing personal information. Whilst sharing data relating to deceased individuals is not treated as personal data under the Data Protection Act, Human Rights Act considerations should be taken into account with regards to whether sharing information could impinge on the rights to a private life for the relatives of deceased individuals.

23. Information Commissioner's guidance advises that if information is being shared in ways that comply with the Data Protection Act, it is also considered likely that the sharing would comply with the Human Rights Act. Nonetheless, nominated individuals or business areas with responsibility for sharing information must ensure that disclosures are compatible with Article 8 of the Convention and seek advice from legal advisers if they have any concerns.

Part 4: Deciding to share information under the powers

Who can share data?

24. It is important that all registration officials understand their roles and responsibilities in relation to information that they may access and share. Responsibility will differ in accordance with the role of the registration official. Decision-making responsibility for sharing data will be in accordance with GRO or local authority policies and guidance. Nominated individuals or business areas will have responsibility for deciding whether information can be shared – e.g. Proper Officers / Registration Service Managers / Superintendent Registrars, Registrar General or GRO Data Unit[6]. This will ensure that consistent approaches are applied by both the GRO and Local Registration Service when considering requests to share information. Data sharing agreements should not be entered into without first consulting these individuals / business areas.

25. All registration officials must adhere to and keep up to date with internal procedural guidance issued by the Registrar General on sharing information. By doing so, they can be confident that they are following the correct procedures when sharing information. Before any data is released by a registration official, written agreement must be obtained from the nominated individual or business areas that have responsibility for sharing information. The written agreement will need to confirm that there is a legal power to share information and confirm exactly what data may be released.

Is there a legal gateway?

26. Prior to sharing information, nominated individuals or business areas with responsibility for sharing information, must be satisfied that there are explicit statutory powers to disclose information and that the disclosure is in accordance with the purposes set out in legislation.

27. The legislative gateway under the Registration Service Act 1953 allows registration officials to share information which they hold in connection

[6] The Local Registration Service will nominate individuals with responsibility for sharing information at a local level. The GRO will be responsible for nominating individuals with responsibility for sharing GRO information.

with their functions with specified public authorities to assist them to fulfil their public functions. This is a discretionary power, with registration officials being able to determine whether or not it is appropriate to share information that has been requested. Examples of the types of information sharing include enabling registration officials to share information more widely within the local authority and across local authority boundaries about the births of children and also any unregistered births. Other examples include providing 'list cleaning' services that would help other departments remove deceased accounts from their systems, therefore enabling them to appropriately carry out their functions whilst at the same time removing correspondence being issued to the families of deceased individuals.

Does the disclosure need to be approved by the Registrar General?

28. In instances where any large amounts of data are requested, prior notification and agreement must be obtained from the Registrar General, unless in situations where the types of exchanges are covered in internal procedural guidance. This will ensure consistency of information sharing across civil registration and prevent any weakening of safeguards.

Criteria for sharing information

29. The main criterion for sharing registration information with specified recipients (as outlined in the primary legislative powers) is that the data must be shared in order to *enable* the recipient to fulfil one or more of their function(s).

30. In addition to satisfying the requirement to enable them to fulfil a function, registration officials should also consider whether:
    - The release of information is compatible with either departmental data sharing principles (for the GRO only) or local authority data sharing procedures;
    - In their role as data controller, registration officials (i.e. those with nominated responsibility for sharing data in accordance with GRO / Local Registration Service policy) consider it appropriate and sensible to take part in the arrangements - for example if there are any perceived conflicts of interest with sharing information;
    - In their own particular circumstances, registration officials with responsibility for data sharing can meet the requirements of the

Data Protection Act and the Human Rights Act when participating in the agreement;

- Registration officials have the resource capacity to release the information;
- The information that has been requested is adequate and not excessive for the purpose for which it has been requested. Only minimum information should be provided in accordance with the specific requirements of the data recipient.

31. In addition to applying data sharing principles, registration officials must adhere to and keep up to date with any guidance issued by the Registrar General (and any local authority policy for the Local Registration Service) to ensure that consistent approaches are being applied when sharing information.

Part 5: Fairness and transparency

Lawful processing

32. Whilst registration officials have discretion to share any information they hold in connection with their own functions under xx of the Act, exercise of that discretion is subject to important limitations. The disclosure of information under (section xx of xx Act) may only be made for the purpose of enabling the recipient to exercise one or more of their functions. Also in order for disclosure to be lawful: the data must not be subject to another express legislative restriction, and the disclosure must be in accordance with the Data Protection Act 1998 and Human Rights Act 1998.

Fair processing

33. The first data protection principle requires, among other things, that organisations must be able to satisfy one or more "conditions for processing" in relation to their processing of personal data. The conditions for processing are set out in Schedules 2 and 3 to the Data Protection Act. Many (but not all) of these conditions relate to the purpose or purposes for which information is intended to be used. Organisations processing data need to meet one or more of the conditions in either Schedule 2 or Schedule 2 and 3 depending on the data being shared. When sharing sensitive personal data the more exacting requirement to meet at least one condition in each schedule applies. Sensitive personal data includes information about an individual's sexual orientation (in the context of civil registration data the existence of an opposite-sex marriage record verses a civil partnership or same sex marriage record will by definition disclose this) and therefore have to meet a condition in both Schedule 2 and 3. For a full list of sensitive personal data see section 2 of the DPA.

34. This will not, on its own, guarantee that the processing is fair and lawful – fairness and lawfulness must still be looked at separately. The Data Protection Act does not define fair processing but provides guidance on the interpretation of this principle in Part II of Schedule 1 to the Act. However, to assess whether or not personal data is processed fairly, registration officials must consider more generally how it affects the interests of the people concerned – as a group and individually.

35. Registration officials are required to ensure that their data sharing practices are fair and transparent. Public authorities will also be required to have fair and transparent processes in place for disclosing and receiving data – e.g. by actively communicating how information is being used via the use of a privacy notice. Registration officials must satisfy themselves that the public authorities' processes are satisfactory for the types of data which is being disclosed before any data is shared and should discuss with the recipients what their arrangements will be. In considering whether to share information, registration officials must also consider whether conditions need to be imposed on the future use and retention of the data by way of data sharing agreements. Any conditions will need to be clearly specified prior to sharing information.

36. Public authorities accessing registration information – e.g. for the purpose of providing services such as digital services, will be expected to ensure that individuals concerned are aware of how their data is being used.

37. In some instances, such as where information is used to data match a large number of individuals, it may be impracticable to send notices to individuals affected by the data sharing. However, registration officials and public authorities will need to comply with requirements of the Data Protection Act in ensuring that data has been shared fairly and lawfully. It will also be necessary to complete standardised records of data shared for audit purposes, detailing the circumstances, what information was shared and an explanation as to why the disclosure took place.

38. The Information Commissioner's Office has produced the following good practice guidance on fair processing including guidance on producing privacy notices to ensure that individuals are aware of which organisations are sharing their personal data, including what it is being used for:
https://ico.org.uk/media/1610/privacy_notices_cop.pdf

Data protection exemptions

39. The Data protection Act includes a number of exemptions which permit disclosure of data notwithstanding the fact that to do so would be incompatible with some of the safeguards provide by that Act. For example some exemptions apply to a number of the data protection principles. Registration Officials should consider the exemptions set out in Part IV of and Schedule 7 to the Data Protection Act and should

contact nominated GRO or local authority individuals with responsibility for data sharing for advice if it appears that an exemption may apply and disclosure could not be made unless it is relied upon.

Data Sharing Agreements

40. "Managing Data" guidance must be followed to determine whether a data sharing agreements[7] are required to provide an audit of data being shared. Formal data sharing agreements will not always be necessary, as some data sharing arrangements will be appropriately covered by routine practices. Guidance states the most appropriate course of action to be followed in accordance with Information Commissioner's Office guidelines.

41. Prior to entering into data sharing agreements, registration officials will need to agree with the public authority that they will take appropriate organisational, security and technical measures to:
    - prevent civil registration data being linked, either itself or with other government data, in order to create any identity datasets or databases.
    - ensure information will be retained securely and deleted once it has been used for the purpose for which it was provided
    - prevent accidental loss, destruction or damage of information
    - ensure only people with a genuine business need have access to the information

42. The data sharing agreements will not be legally binding, however will be expected to include details of:
    - The purpose of the data sharing arrangement
    - The respective roles, responsibilities and liabilities of each party involved in the data share
    - The legal basis for exchanging information
    - The accuracy of the data – ensuring that the recipient is aware that registration data is only as accurate as at the time it is captured and will be treated as such
    - Precise details of what exact data is required to enable them to perform the function for which it is requested
    - Restrictions on sharing certain categories of data – i.e. adoptions and gender recognition data
    - Restrictions on any onward disclosure of information - if applicable

[7] Data Sharing Agreements may also be known by other names such as Memorandums of Understanding

- Information handling responsibilities, including details of any data processors or subcontractors
- Conditions for data processing, including whether data subjects are aware of how their data is being shared, including the methods of sharing and whether they are likely to object to it
- Process and methods of exchange
- Standards and levels of expected operational service
- Reporting arrangements, including any reporting in the event of any data loss and handling arrangements
- Termination arrangements
- Issues, disputes and resolution procedures
- Information on data security, data retention and data deletion
- Review periods
- Individuals' rights – procedures for dealing with access requests, queries and complaints
- Any costs associated with sharing data
- Sanctions for failure to comply with the agreement or breaches by individual staff

43. The above list is not exhaustive. For more detail on data sharing agreements see https://ico.org.uk/for-organisations/guide-to-data-protection/ or contact your local data protection adviser.

44. Data sharing agreements should contain details of sanctions that will apply to recipients of information who are found to be processing data unlawfully or inappropriately. These sanctions will include, but are not limited to:

    (a) Public authorities ceasing to receive information from registration officials. Regulations may be made to remove the organisation from the list of bodies able to share information under the power;
    (b) Registration officials considering whether it is necessary to report the recipient and incident to the Information Commissioner's Office who will consider whether penalties are applicable;
    (c) Registration service officials determining whether any misuse of public office offences have been committed, and if so, to take any necessary action where this has occurred;
    (d) Public authorities found to be in breach of any data sharing agreements needing to formally re-apply for accessing data again in the future;
    (e) Public authorities that have previously breached a data sharing agreement only being granted access to information again if registration officials are satisfied that any security or

other issues have been resolved to reduce the risk of any further issues occurring in the future.

45. Both the General Register Office and Local Registration Service will be required to maintain up to date lists of their individual data sharing agreements for audit purposes.

46. Public authorities will need to satisfy themselves that they are complying with the Data Protection Act and should be advised to seek their own legal advice regarding data sharing following any agreements to access registration information.

Privacy Impact Assessments

47. Privacy Impact Assessments are a useful tool which can help registration officials identify the most effective way to comply with their data protection obligations and meet individual expectations' of privacy. All government departments entering into data sharing arrangements under these powers must conduct a Privacy Impact Assessment and to publish its findings. The Information Commissioner's Conducting Privacy Impact Assessments code of practice provides guidance on a range of issues in respect of these assessments, including the benefits of conducting privacy impact assessments and practical guidance on the process required to carry one out.

48. Privacy notices describe all the privacy information you make available or provide to individuals about what you do with their personal information. Privacy notices must be published and made available to the public in line with fairness and transparency principles in the Information Commissioner's privacy notices code of practice[8] and data sharing code of practice. The Information Commissioner's privacy notices code of practice provides guidance on the content of these notices, as well as where and when to make them publicly available.

49. Registration officials entering into new data sharing arrangements should refer to the following guidance issued by the Information Commissioner on Privacy Impact Assessments which includes screening questions (Annex one: p33 https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf) to determine whether a Privacy Impact Assessment is required.

[8] https://ico.org.uk/media/for-organisations/documents/1610/privacy_notices_cop.pdf

Part 6: Governance

Application process

50. A formal application process and audit trail of decisions will need to be in place to ensure that informed decisions on data sharing can be made by registration officials at the right level in the organisation. Whilst the process to be followed may differ in accordance with whether the applicant is applying to the General Register Office or the Local Registration Service, each application process should be consistent with the principles below.

51. Questions that should form part of the application process include:
    - What information is being requested?
    - For what specific purpose and public function is the information being requested?
    - How does the data exchange enable the recipient to perform their functions?
    - Have any legal gateways been identified? If so, are there any restrictions on what can be disclosed?
    - What exact data items are required – e.g. names, dates of birth, gender?
    - Has the recipient of the data any legal obligations to provide personal data they hold to any other bodies?
    - How regularly and in what volume is it proposed to share the data?
    - High-level details of security provisions that are in place/will be put in place to safeguard data exchange, handling and retention?
    - Does the proposal suggest transferring information outside the UK/EEA or storage of information on servers outside the UK or in the cloud? If so, what security measures are taken to ensure data security?
    - Is there a time-limit suggested for using the data and if so how will the data be deleted?
    - Is funding available to pay for costs incurred with the data share?
    - Will the data subjects be aware that their data is being shared – e.g. via a privacy notice?
    - Has a Privacy Impact Assessment been conducted/findings of a Privacy Impact Assessment?
    - Are there any other benefits (including financial) of the data exchange for the receiving party or any other public body?

- Implications of not sharing information – e.g.
  - Public finances or commercial projects are at risk
  - The Government is in direct contravention of the law
  - The Government's reputation is at risk
  - The Government's ability to deliver services is at risk
  - The Government is not able to fulfil its functions

52. In completing applications, the following key issues need to be satisfied and understood:
    - All parties must be clear on the tangible benefits (including financial) that are expected from the information sharing, who will receive them and how they will be measured.
    - The purpose of the information sharing needs to fall within the purposes outlined in legislation – i.e. providing information to a public authority for the purpose of enabling them to fulfil one or more of their functions.
    - Only minimum data will be provided to meet a specific function.
    - Information sharing must be physically and/or technically possible and be compliant with the Data Protection Act 1998, Human Rights Act 1998.
    - Strict compliance with security provisions to safeguard against any misuse or loss of data, including having secure methods in place for transferring data.

Data standards and data accuracy

53. The General Register Office and Local Registration Service hold data in a number of different formats. When considering sharing information it is essential that every effort is made to ensure that data is not affected once transferred. This will help ensure that individuals are not adversely impacted by any exchanges – e.g. prevented from accessing a service where there are issues with data held by a recipient as a consequence of the data exchange.

54. It is also important that checks are made on the accuracy of data prior to transferring data. In instances where issues arise following the transfer of data, procedures need to be in place to allow for inaccurate data to be corrected by all bodies holding the information. Registration officials will need to be aware of the correct procedures to follow with regards to correcting inaccurate data held on their own systems, including alerting data protection officers and other identified teams to ensure data is corrected where held on other systems.

Compliance

55. The Registrar General will work with the National Panel for Registration when producing any associated guidance and on any measures to ensure compliance with this Code of Practice, for which he / she has responsibility.

56. Where it becomes evident that regard is not being given to the Code, the Registrar General will work with the National Panel for Registration on any measures to ensure compliance, for which he has responsibility. In instances where data protection issues are identified, the Information Commissioner's Office will be notified at the earliest opportunity.

57. Any general questions with regard to compliance should be taken up with the GRO in the first instance.

58. The Registrar General has responsibility to review the Code on an annual basis. The National Panel for Registration will be consulted when reviewing the Code to ensure any amendments support the delivery of the Local Registration Service and their own data sharing arrangements in line with the Code.

UK Statistics Authority

Data Sharing Code of Practice and Accreditation Criteria: Research

---

Code of Practice and Accreditation Criteria for access to data for research purposes

Date: 20 October 2016

Research: Data Sharing Code of Practice and Accreditation Criteria

Contents

Part 1: About the Code of Practice

1. The Act requires three groups of people to have regard to the principles set out in this code of practice:
    - Data holding public authorities in disclosing data for processing, for subsequent research purposes;
    - Processors involved in the processing of this data, whether that processing be concerned principally with the linkage or de-identification of data, or the storage and provision of secure access to the de-identified data; and
    - Individuals to whom de-identified data is made available for research.

2. The eight principles below are intended to collectively ensure that the processing and provision of de-identified data under the Act is ethical and legal, and done in a way that ensures information that relates to an individual (regardless or not of whether this information identifies the individual) is appropriately protected. All parties involved in the disclosure, processing or use of data under this legislation are required to adhere to these principles in performing their function under the legislation.

3. The Act further requires that all persons or organisations involved in the processing or use of data secure accreditation appropriate to the functions they seek to fulfil under the legislation. Details of the conditions for accreditation are set out under the accreditation criteria.

4. This document has been prepared in accordance with these requirements. In drawing up the code and the accreditation criteria, the Authority has had regard to, inter alia, the:
    - Information Commissioner's Data Sharing code of practice (2011)
    - Information Commissioner's Anonymisation Code of Practice (2012)
    - Information Commissioner's Conducting Privacy Impact Assessments Code of Practice (2014)
    - Information Commissioner's Privacy Notices Code of Practice (2016)
    - Statistics and Registration Service Act 2007
    - Code of Practice for Official Statistics (2009)
    - Data Protection Act 1998
    - Report of the Administrative Data Taskforce (2012)
    - Cabinet Office Open Data White Paper (2012)

5. The code of practice consists of eight principles, set out below, which apply to all stages in the processing as described in this document, and to the use of de-identified data made available through this gateway. Since there are a number of different ways in which data may be safely and securely processed and used this document does not attempted to provide detailed

guidance on any aspect of the handling or use of data under this legislation. It is instead incumbent on individuals or organisations using this gateway to develop, implement and be able to clearly demonstrate practices and arrangements that fully adhere with the principles described below.

Part 2: Understanding the power

6. Through the Digital Economy Bill [Act 2017] (hereafter the Bill [Act]) the UK Parliament has enacted legislation that facilitates the linking and sharing of datasets held by public authorities for research purposes. The legislation helps to position the UK at the forefront of the international science landscape and supports a number of direct public benefits:
   - increasing the availability of varied and high-quality data for researchers within and outside government will drive improvements in the evidence base available to policy and other key decision-makers;
   - facilitating the linkage of datasets held by two or more public authorities in controlled environments offers increased opportunities for new insights into the social and economic challenges that citizens and businesses face;
   - helping researchers and policy-makers build a better understanding of how people live their lives, their patterns of need and use of different services and the resultant outcomes, to support the design and delivery of more effective and efficient public services.

7. The legislation provides certainty and clarity for public authorities and researchers concerning what data can be made available for research purposes and the conditions under which that data can be made available. This will reduce the delays and inconsistent approach to releasing publicly-held data for research purposes, helping to ensure that the economic and social benefits associated with research are more easily realised.

8. To ensure data are processed and made available in a safe and secure way the legislation sets out six conditions under which this can take place. It also sets out sanctions for those failing to observe the conditions described in the legislation or the principles governing disclosure described below.

9. Section 56 of the Bill [Act] creates a gateway to enable public authorities to make data available to researchers for research that is in the public interest using a trusted third party model. Under this model, a data holding public authority discloses identifiable data to an accredited third party (or the public authority itself acting in this capacity), who is then responsible for processing the data (that is, linking, de-identifying, storing, making data securely available or related procedures) before the de-identified data are made available to a nominated researcher. Section 56(3)-(8) of the Bill [Act]

sets out six conditions under which information can be disclosed under this power, specifically that:

(1) Data must be de-identified before they can be made available so that the data do not directly identify individuals and are not reasonably likely to lead to an individual's identity being ascertained;

(2) The parties involved in processing the data must implement and maintain appropriate safeguards to minimise the possibility that identifying data might be accidentally or intentionally disclosed;

(3) The data is made available to the researcher either directly by the person(s) involved in the processing of the data, or, once data are suitably processed, the data holding public authority;

(4) The research for which the de-identified data are being made available is in the public interest and has been assessed as such through an accreditation process;

(5) The researcher(s) and all persons involved in processing the data are accredited for these functions; and

(6) Public authorities disclosing data to trusted third parties for processing and making de-identified data available for research purposes, and trusted third parties involved in processing information for the same purpose, have regard to this code of practice.

10. Section 61 identifies the UK Statistics Authority (hereafter the Authority) as the body responsible for overseeing the accreditation processes set out in the Act.

11. Section 60(1) of the Bill [Act] establishes the requirement that the Authority prepares and publishes a code of practice concerning the disclosure, processing, holding and use of information under this gateway. The Authority must consult publicly before issuing or reissuing this code, and must lay the code before the UK Parliament and the legislatures of the devolved administrations in Scotland, Wales and Northern Ireland.

12. The Bill [Act] further obliges the Authority to publish a set of criteria that individuals, organisations and research projects must meet before being accredited for any of the functions set out in the legislation.

Part 3: Principles governing the disclosure of data

Principle 1: Legal

13. Data can only be disclosed to processors (for the purpose of subsequently making de-identified data available to researchers) where expressly permitted through the meeting of the six conditions set out at section 56 of the Digital Economy Bill [Act 2017], or through appropriate secondary regulations, as established by the Westminster Parliament or the legislatures of the Devolved Administrations in Scotland, Wales and Northern Ireland. Data holders, processors and researchers must also ensure they adhere to the legal requirements set out in the Data Protection Act 1998 and Part 1 of the Regulation of Investigatory Powers Act 2000, and are expected to have regard to best practice on privacy impact assessments and privacy notices, as established in the ICO's Conducting Privacy Impact Assessments Code of Practice and Privacy Notices Code of Practice.

Principle 2: Accreditation

14. All accredited persons and the research project must remain accredited for the duration of the project and at all times when processing, accessing or using the data, and must therefore observe the requirements for the maintenance of accreditation (such as training obligations). Data holders and accredited processors are also required to ensure that where they disclose or make available data to other processors or researchers it is done for the specific purposes set out in the Bill [Act] and only to a person that is accredited for the function they are fulfilling. The UK Statistics Authority will ensure that it exercises its accreditation function in a way that is free from the influence of organisational, political or personal interests, and that accreditation applicants (or those whose accreditation is suspended or removed) have recourse to appropriate appeals mechanisms.

Principle 3: Data security and confidentiality

15. All parties and persons disclosing, making data available, processing or using data under the provisions set out in the Bill [Act] must ensure they do so in a way that never compromises the confidentiality of personal information. Appropriate safeguards must therefore be established and maintained at all stages and by all parties and persons involved in the disclosure or processing of data and their use for research purposes. Before providing accredited researchers access to data, processors must ensure the data has undergone a process of disclosure control that is commensurate and proportionate with the sensitivity of that data. All persons handling data must ensure the integrity of these safeguards is maintained by proactively identifying privacy and security risks and regularly

reviewing safeguards and security solutions to ensure they continue to meet the challenges posed by evolving technologies.

Principle 4: Public interest

16. Data obtained under this legislation must only be disclosed, processed and used for the purpose of supporting research in the public interest. Research in the public interest is research that will, for example:
    - provide or improve evidence bases that support the formulation, development or evaluation of public policy or public service delivery;
    - guide critical decision-making with anticipated impacts on the UK economy, society or quality of life of people in the UK;
    - significantly extend existing understandings or social or economic trends or events, either by improving knowledge or challenging accepted analyses; or
    - replicate, validate or critically analyse existing research (including official statistics) in a way that leads to improvements in the quality, coverage or presentation of existing research.

17. The UK Statistics Authority has set out further information concerning the criteria for determining whether research is in the public interest under the criteria for the accreditation of research projects, set out below.

Principle 5: Ethical

18. All parties must ensure that they observe the highest ethical standards when sharing, processing or making use of data under this gateway. They must ensure that the unique ethical challenges presented by using data collected for operational reasons and held by public authorities are reflected and accounted for in the discharging of each of the functions described within the Bill [Act]. This will involve, principally, ensuring the appropriate consideration of issues of privacy, identifying and minimising the risks of re-identification, and considering risks appropriate to the type, scale and sensitivity of the data being disclosed or made available. It may also require reflecting on the risks and limits of new technologies, oversight practices and adherence to recognised methodological and quality standards, legal obligations and public acceptability.

Principle 6: Proportionality and minimised burdens

19. Data must be disclosed or made available in a way that ensures the burdens and costs of doing so are proportionate to the anticipated benefits of the proposed research, whether those burdens and costs are accrued by the public authority acting as a data holder, the public authority or trusted third party acting as a processor, or the researcher(s). A researcher should ensure that in seeking to secure access to data held by public authorities he or she has assessed, in so far as he or she is able, suitable, less burdensome alternatives and is satisfied that no alternatives exist or that the financial or quality costs of securing data from other sources would be prohibitive.

Equally, data suppliers are required to provide data as efficiently as possible, and to ensure that any cost recovery charges are proportionate to work undertaken specifically for the purpose of releasing data for specified research projects.

Principle 7: Retention and onward disclosure

20. Third party data processors can only retain pre-processed, identified data for a limited time. The UK Statistics Authority will set out this period as part of the accreditation process and in accordance with the nature of the data, good practice guidelines and any other relevant considerations. Data processors will be able to apply to the Authority for an extension of this period where there is a clear research rationale for doing so (such as in the case of longitudinal studies).

21. Processors who store the de-identified data may make that de-identified data available to other researchers and for other research projects within this time period only where the following criteria are met:
    - the data supplier has agreed to the processor making the de-identified data available to additional individuals and / or for additional research projects;
    - the processor remains fully accredited for its disclosure function; and
    - the researcher and the research projects are fully accredited for the use of these data.

22. In line with the requirements set out under Principle 2, under no circumstances should data be disclosed, made available in de-identified form or passed to any parties who are not suitably accredited.

Principle 8: Transparency

23. All parties should adopt a commitment to transparency, where possible, to maximise the potential public value of research facilitated by access to public data. Researchers should engage core stakeholders on the findings of the research drawn from these data, and ensure that research findings are made freely available to the public. Data supplying public authorities and processors may also choose to publish information about the data they are making available, the rationale and purpose of doing so, and any restrictions and safeguards associated with the processing and use of those data. Considerations of whether or not to publish such information should be balanced with security or other considerations where the risks of publishing such information would outweigh the potential public benefits. In its accreditation capacity, the UK Statistics Authority may also chose to publish details on accreditation applications and outcomes, including the outcome of any appeals process, in accordance with its statutory responsibilities.

Part 4: Accreditation Criteria

Accreditation of processors

24. The disclosing and provision of data held by public authorities for the purpose of conducting research in the public interest, as set out in the legislation, is conditional on the data being processed by an accredited processor. A processor must be accredited for one, or both, of two functions, specifically:
    (i) the linking, matching and de-identifying of data (hereafter referred to as the preparation of de-identified data); and/or
    (ii) the storing and provision of access to data (hereafter referred to as the provision of de-identified data).

25. Any person(s) involved in either the preparation or provision of data under this legislation must be accredited for the appropriate function (or both), as appropriate. Accreditation documents will clearly state for which of these functions the processor has been accredited. The UK Statistics Authority will also publish details of accredited processors, along with details of which function(s) the accreditation covers.

26. In some cases, the processor could be the public authority whose data has been requested if they have the necessary expertise. To maintain standards and consistency throughout the accreditation process public authorities processing their own data for accredited research purposes – or indeed, linking and matching their data to that held by another public authority – must be appropriately accredited for the processing function they are performing.

27. By default, an accredited processor will retain accredited status for five years, or for as long as they continue to meet the conditions for accreditation set out below. After this time an accredited processor will need to apply for a renewal of its accredited status. From time to time emerging data threats and challenges may make it necessary to change the conditions required for accreditation as a processor. In such circumstances the UK Statistics Authority may decide to provide notice of its intention to suspend and reassess the accreditation status of processors.

28. To secure accreditation processors must meet the following conditions:

The processor must be based within the territorial jurisdiction of the UK

29. To ensure processors are legally accountable for the work they carry out under the legislation only processors based in the UK are eligible for accreditation. The processor must in addition provide a guarantee, at the

point of accreditation, that it will carry out all of its processing within the UK. The processor must be able to provide evidence on request that this is the case in order to maintain its accredited status.

The processor must meet current and appropriate cross-government standards for the secure holding of sensitive data

The processor must have appropriate skills and experience

30. The processor must ensure that its staff have the necessary skills and experience to undertake the work required to the standards required, as appropriate for the processing function for which accreditation is sought. Staff involved in the preparation of data must have received training and be able to demonstrate their understanding of the linking, matching, and de-identification of data in a safe way; those involved in the provision of data must be able to demonstrate their experience and capacity to store and make de-identified data available safely. Individuals responsible for any aspect of the processing of the data should also have security clearance appropriate to the nature of the data they are handling.

31. The processor must agree to maintain a list of all those individuals who meet these requirements, and to ensure that individuals are only involved in aspects of the processing for which they are suitably experienced and trained and that only these individuals have access to data provided by the public authority. A processor must also agree to ensure that all individuals involved in any aspect of the processing have signed a declaration to say that they understand their responsibilities.

The processor must make use of appropriate technical infrastructure

32. The processor must make use of suitable data infrastructures to enable it to securely link, match, de-identify data, store and make de-identified data available, as appropriate for the specific function(s) the processor is fulfilling.

The processor must agree to publish and maintain appropriate data policies

33. At the point of application the processor must present, and maintain for as long as they wish to remain accredited, a set of detailed documents that demonstrate, to the Authority's satisfaction, that the processor will meet the requirements for handling, storing, protecting and destroying data it processes for research under this legislation. Specifically:
    - A Secure Environments Policy that ensures that the physical environment and processes meet the requirements to hold sensitive data. For processors seeking accreditation for the provision of data these policies must cover the operation of the secure data access facility where researchers can access data. Secure data processing facilities must be suitably accredited in line with cross-government security standards;
    - A Major Incident Protocol related to data security and privacy breaches;

- A De-Identifying Data policy;
- A Data Retention and Destruction policy; and
- A Data Confidentiality Breaches policy.

34. The processor must ensure that adequate data processing agreements are in place for any data they receive from public authorities before they process that data. The processor must also agree to abide by any additional policies and procedures the UK Statistics Authority in its accreditation capacity may develop and set out from time to time. The Authority will provide appropriate notice where it intends to introduce new policy requirements.

The processor must comply with UK law

35. The processor must undertake to comply with all aspects of UK law set out in primary and secondary legislation, whether enacted by the Westminster Parliament or, where processing is taking place within the jurisdiction of a devolved administration, by the appropriate devolved legislature. Processors must, in particular, ensure they comply with the legal requirements set out in the Data Protection Act (1998), the Human Rights Act (1998), the Statistics and Registration Service Act (2007), and Part 1 of the Regulation of Investigatory Powers Act (2000). Compliance may be assessed by an audit and is a central condition for the maintenance of a processor's accredited status.

The processor must agree to its inclusion on a public register

36. The UK Statistics Authority is required to maintain a public register of accredited persons. Any persons seeking accreditation for processing under this legislation must therefore agree to their inclusion on this register.

The processor must consent to being audited

37. In order to discharge its duty of oversight and ensure processors continue to meet these requirements the UK Statistics Authority may, from time to time, decide to undertake an audit of accredited processors. Processors are required to consent to be audited during its accreditation application, and must fully comply with any audit that takes place in order to maintain its accredited status.

The processor must commit to having regard to the Code of Practice

38. The processor must undertake to adhere to the principles set out in the code of practice when fulfilling any of its processing functions. Compliance may be assessed by an audit and is a central condition for the maintenance of a processor's accredited status.

Withdrawal of accreditation

39. Accreditation may be suspended or withdrawn from a processor accredited for the preparation or provision of data for any or multiple of the following reasons:

- Failure to have regard to the code of practice under section 60 of the Digital Economy Bill [Act 2017];
- Conviction for offences under the Data Protection Act;
- Penalties imposed by the Information Commissioner's Office relating to processing under section 56 of the Digital Economy Bill [Act 2017];
- A reported or suspected data breach
- Failure to meet accreditation requirements;
- Refusal to provide, or withdrawal of, the processing service for which it has been accredited;
- Refusal to be audited, or obstruction of the auditing process; and/or
- Charging fees for processing, other than those ordinarily permitted for cost-recovery purposes.

Other considerations

40. The UK Statistics Authority will provide further guidance on the procedures and processes governing the accreditation of processors for the purpose of preparing or providing access to data under the legislation.

Accreditation of researchers

41. Researchers undertaking research using data provided under the gateway set out in part 5, chapter 5 of the Digital Economy Bill must secure accreditation by meeting the following conditions:

The researcher must provide evidence of suitable research qualifications and/or experience

42. To ensure a researcher has the necessary skills to make suitable use of the data they must be able to demonstrate through example(s) the following skills;

- Evidence gathering
- Literary review
- Interpretation & analysis of data
- Drawing conclusions
- Presentation of results

The researcher must agree to undertake compulsory training

43. The UK Statistics Authority (or its partners) may choose to provide training on the safe handling of the data and disclosure control rules for the outputs to ensure researchers are fully aware of their obligations, and to therefore minimise the risk of disclosure of personal information. Researchers must agree to undertake any training required by the Authority. Failure to undertake this training may constitute grounds for the suspension or removal or accreditation until the training is completed.

The researcher must agree to their inclusion of a public record

44. The UK Statistics Authority is required to publish a register of accredited researchers. The Authority may also chose to publish a high-level overview of accredited research projects and accredited researchers associated with these projects. Researchers must agree for these details to be published on the register unless the Authority agrees that there are exceptional reasons not to do so.

The researcher must sign a declaration

45. The researcher must sign a declaration confirming that they have understood their responsibilities and will abide by the conditions imposed upon them, including protecting the confidentiality of information they access under the legislation.

Withdrawal of accreditation

46. Accreditation may be suspended or withdrawn from an accredited researcher for any or multiple of the following reasons:

- Failure to have regard to the code of practice under section 60 of the Digital Economy Bill [Act 2017];
- Failure to disclose information that could materially affect the accreditation process (such as a previous conviction under the Digital Economy Bill [Act] s.58(5) or 59(4); or under the Data Protection Act), or dishonestly completing the application form;
- Failure to adhere to the terms of any written data access agreement between the data holding public authority and the researcher;
- Acting unlawfully in relation to activities for which he or her is accredited;
- Bringing the accreditation scheme into disrepute;
- Failure to undertake or complete the appropriate training; and/or
- Deliberately facilitating or, through negligence, enabling access to the data by a non-accredited person.

Other considerations

47. The UK Statistics Authority will provide further guidance on the procedures governing the accreditation of researchers under the legislation, including any training that is a condition of accreditation. In addition to the criteria set out above, applicants should note the following considerations:

- Accreditation as a researcher will be for default period of five years. Researchers are required to renew their accreditation once this term has expired;
- Applicants will be asked to include any relevant information which they think adds or detracts from the application. Steps will be taken during the application process to verify the identity of the applicant;
- Researchers only need to be accredited once (subject to renewal requirements), but every project requires approval. In line with principle 2 of the code of practice accredited researchers can only use data for the purpose of an accredited research project and that has been processed by an accredited processor;
- If the applicant is working towards acquiring the level of skills stated above they may be eligible to apply for provisional accreditation where a fully accredited researcher has agreed to direct, supervise and take responsibility for all work undertaken by the applicant, and on condition the applicant meets criteria 2 to 4 set out above; and
- A researcher who is refused accreditation, or who has their accreditation suspended or removed will have a right to appeal.

Accreditation of research projects

48. Research projects making use of data provided under the gateway set out in part 5, chapter 5 of the Digital Economy Bill must secure accreditation by meeting the following conditions:

The research must comply with UK law

49. The research must comply with all aspects of UK law set out in primary and secondary legislation, whether enacted by the Westminster Parliament or, where processing is taking place within the jurisdiction of a devolved administration, by the appropriate devolved legislature. The application must demonstrate to the satisfaction of the UK Statistics Authority that the proposed research project will meet the data protection principles as set out in the Data Protection Act and monitored by the Information Commissioner's Office.

The research project must be in the public interest

50. The legislation makes it a condition of the disclosure of data that the research for which the data is disclosed is in the public interest. For the purposes of accrediting research projects the UK Statistics Authority interprets public interest in the same way as 'public good', as set out in the Statistics and Registration Service Act 2007. To secure accreditation the primary purpose of a research projects must therefore be to serve the public interest in one or more of the following ways:

    - to provide an evidence base for public policy decision-making;
    - to provide an evidence base for public service delivery;
    - to provide an evidence base for decisions which are likely to significantly benefit the economy, society or quality of life of people in the UK, UK nationals or people born in the UK now living abroad;
    - to replicate, validate or challenge existing research, including official or National Statistics;
    - to significantly extend understanding of social or economic trends or events by improving knowledge or challenging widely accepted analyses; and/or
    - to improve the quality, coverage or presentation of existing research, including official or National Statistics.

The research and its results must be transparent

51. The intention and anticipated impact of the research should be set out to the satisfaction of the UK Statistics Authority as part of the application.

52. When the project is complete, all results or outcomes of the research must be made freely available in a way that could reasonably be expected to be permanent. The public authority which is the source of the data should be acknowledged to allow others to verify the research. The applicant must also set out a clear commitment to engage with core stakeholders on any useful findings from the research in order to maximise the public benefit.

The research must have ethical clearance from a recognised body

53. The research must be reviewed and approved by a body that is suitably qualified and appropriate to review the ethical considerations of the proposed research (such as a university ethics committee or an independent body). In addition to demonstrating how the proposed research serves the public interest and is fully compliant with UK law (see above), applications will need to demonstrate that:

    - Potentially disclosive information will be stored confidentially and securely;
    - Issues of consent have been appropriately considered and addressed;
    - The risks and limits of new technologies have been considered;

- The research plan provides for human oversight to ensure the methods are consistent with recognised standards of integrity and quality;
- The views of the public have been considered in light of the data used and the perceived benefits of the research;
- The access, use and sharing of data is transparent, and is communicated clearly and accessibly to the public.

The data requested must be appropriate for the research that is proposed

54. The application must demonstrate that the data requested is suitable for the research that is proposed, and that the data requested does not exceed the requirements of the research project.

All researchers must be named and accredited

55. The project application must name all the researchers who will be accessing the data. No researcher may access the data before they are accredited under this scheme. When researchers leave or are added to the research project the change must be communicated to the UK Statistics Board.

Withdrawal of accreditation

56. Accreditation may be suspended or withdrawn from an accredited research project accredited for any or multiple of the following reasons:
    - Failure to have regard to the code of practice;
    - The research project is no longer covered by ethical approval;
    - Information comes to light, or the research project changes, so that the project can no longer be considered to be in the public interest;
    - A reported or suspected data breach;
    - A court ordered that the research be halted.

Other considerations

57. The UK Statistics Authority will provide further guidance on the procedures and processes governing the accreditation of research projects under the legislation. In addition to the criteria set out above, applicants should note the following additional considerations:
    - The application should include an indication of how long data will be needed for. To comply with the Data Protection Act, and in accordance with principle 7 of the Code of Practice, data will be destroyed once it is no longer needed for the accredited research project, unless an extension of retention has been granted.

- A project can be accredited for a maximum duration of five years, after which the research will require reaccreditation if ongoing access to the data is required.
- A research project can remain accredited even where accreditation is withdrawn from the organisation processing data for the project, or from the researchers carrying out the project, provided the research project does not breach any of the criteria set out above.

UK Statistics Authority

Data Sharing Statement and Code of Practice: Statistics

Statement of Principles and Procedures and Code of Practice for Changes to Data Systems

Date: 20 October 2016

Contents

Statement of Principles and Procedures

Part 1: About the Statement

1. The legislation requires that the UK Statistics Authority prepare, consult on and publish a Statement of Principles and Procedures governing the way we will use the framework for access to data. We are required to consult publicly before issuing or reissuing this statement, and to lay the statement before the UK Parliament and the devolved legislatures.

2. In preparing this statement we have had regard to, inter alia, the:
   - Information Commissioner's Anonymisation Code of Practice (2012)
   - Information Commissioner's Data sharing code of practice (2011)
   - Information Commissioner's Conducting Privacy Assessments Code of Practice (2014)
   - Information Commissioner's Privacy Notices Code of Practice (2016)
   - Statistics and Registration Service Act (2007)
   - Code of Practice for Official Statistics (2009)
   - Data Protection Act (1998)
   - ONS Respondent Charter for Surveys of Households and Individuals
   - ONS Respondent Charter for Business Surveys
   - Government Security Policy Framework
   - The Ethical Principles of the National Statistician's Data Ethics Advisory Committee
   - Responses to the Cabinet Office consultation, Better Use of Data in Government (2016)

3. This statement complements and is consistent with the principles and expectations set out in these documents. The principles and procedures outlined in this document apply to all the ways we access and share data, including onward disclosure to the statistical departments of the devolved administrations.

Part 2: Understanding the power

4. Statistics are a vital public good for the information age – the quality and range of official statistics provide key decision-makers in Government, business and beyond with crucial insights into the UK's society and economy. Official statistics also play a vital role in supporting a healthy democracy by enabling individuals to hold their elected representatives to account. Producing high quality official statistics requires sophisticated, robust methodology and an appropriately skilled statistical workforce. But it also requires a legal framework that empowers statistical producers to collect and process the data on which National and official statistics and statistical research are based. Such a framework needs to recognise:
    - that the way data are produced will continue to change in the future;
    - that data useful for the production of statistics and for statistical research is held by an increasing number of public and private bodies in ever larger quantities, and that the proliferation of useful data sources will continue in the future;
    - the need for statistical producers to be able to understand the data they are using (metadata) so they can take advantage of the growing potential uses of these data; and
    - that the proliferation of data and data holders means greater variation in the quality of data, and that statistical producers therefore need tools that help them to understand the quality of that data and to determine the feasibility of their use in the production of official statistics.
    - that ensuring the increased availability of data to researchers does not impact negatively on citizens' privacy means ensuring those who collect and handle data implement robust privacy-enhancing measures.

5. The Statistics and Registration Service Act 2007, as amended by the Digital Economy [Bill], creates a legal framework providing the UK Statistics Authority and its executive office, the Office for National Statistics (collectively hereafter "the Authority"), access to data held by public authorities and private undertakings to support the Authority's statistical functions. The legislation provides for data suppliers to be required to consult the Authority before changes to data collection are made in order to protect the security of data supply, as well as the accuracy and reliability of statistics derived from these data sources. To support the production of devolved statistics, the legislation permits controlled disclosure of data to the statistical departments of the devolved administrations in Scotland, Wales and Northern Ireland, with the consent of the data supplier. The legislation obliges the Authority to observe the very highest standards of data security, confidentiality and transparency, and sets out strict penalties for those who misuse data collected for statistical purposes.

Part 3: Principles and Procedures

6. The Authority has established principles and procedures to ensure that we:
   - exercise our statutory responsibilities in a fair, proportionate and accountable way, with due regard for key principles of privacy and appropriate degrees of internal and external scrutiny;
   - work in a transparent manner with data suppliers, civil society and the general public, responding to any concerns or opportunities as they arise; and
   - reinforce our full accountability to the UK Parliament and the devolved legislatures in exercising our statutory responsibilities.

7. We will only seek access to data for the purposes of fulfilling our statutory responsibility to produce official statistics and undertake statistical research that meets identifiable user needs for the public good. In exercising our powers we will adhere to the following six principles, collectively intended to ensure that the highest ethical and legal standards apply across the full statistical life-cycle, and to provide public assurance and maintain confidence in the trustworthiness and quality of our statistics. These are outlined below.

Principle 1: Confidentiality

8. The Code of Practice for Official Statistics requires that "private information about individual persons (including bodies corporate) compiled in the production of official statistics is confidential, and should be used for statistical purposes only" (Principle 5).

9. We are committed to maintaining the confidentiality of data at all times, in accordance with Principle 5 of the Code of Practice for Official Statistics. In addition to the strong protection provided by the law, we will ensure that appropriate security controls are applied, and we will observe the highest standards in disclosure control to ensure personal data remains protected and secure at all times. We will regularly assess our security infrastructure and procedures to maintain the integrity of, and confidence in, these safeguards.

Principle 2: Transparency

10. As part of our statutory reporting obligations we are committed to publishing information on how we exercise our statutory responsibilities and obligations in respect of access to sources of data for statistical and research purposes. To help data suppliers and data subjects to understand the ways in which their data are used, and the privacy and security safeguards around the use of these data, we commit to make details of data access requests, requirements, and agreed arrangements publicly available by default. In some exceptional cases this degree of transparency may be

inappropriate;[1] in such instances we undertake to obtain and take into account the data supplier's advice where we are aware, or have been made aware, that such reasons may exist, before deciding whether to (or the extent to which we will) publish details of data access requests, requirements or arrangements. This commitment applies equally to any details we publish in documents we are required or choose to lay before Parliament.

Principle 3: Data sharing, ethics and the law

11. The Code of Practice for Official Statistics requires that "statistical methods should be consistent with scientific principles and internationally recognised best practices, and be fully documented. Quality should be monitored and assured taking account of internationally agreed practices." (Principle 4).

12. Data access arrangements will meet all legal obligations arising from the Data Protection Act (and other legislation, as appropriate). We will further ensure that data access arrangements observe the highest ethical standards, ensuring at all times that these arrangements support the delivery of National and official statistics, and statistical research, that serve a clear public interest. We will ensure that data access arrangements adhere to recognised standards of methodological integrity and quality; address issues of privacy and transparency; suitably consider the risks and limitations of new technologies and data collection methods; and be subject to appropriate scrutiny, oversight and monitoring.

13. As part of this process, we will have regard to best practice on privacy impact assessments and privacy notices in the establishment of data access arrangements, as covered by the ICO's Conducting Privacy Impact Assessments Code of Practice and Privacy Notices Code of Practice.

Principle 4: Integrity

14. The Code of Practice for Official Statistics requires that "at all stages in the production, management, and dissemination of official statistics, the public interest should prevail over organisation, political or personal interests" (Principle 3).

15. We will use our statutory functions and responsibilities in ways that are free of the influence of organisational, political or personal interests, ensuring that we take decisions on the data sources we seek to access only on the basis of a sound statistical rationale, identifiable user needs, and a clear public interest. We will only seek access to data where we are satisfied that the data may be of sufficient quality and coverage to support the

[1] For example, where the publication of such details may be prejudicial to wider public or commercial interests, such as national security, the prevention or detection of crime or where publishing the information would significantly damage the market position of a data supplier.

production of high quality statistical and research outputs. Before securing access to data held exclusively by public authorities or private undertakings under the statutory powers conferred upon us, we will also ensure that we have assessed known viable alternatives, particularly where publicly-available equivalent sources would serve as suitable substitutes.

Principle 5: Proportionality, fairness and minimised burdens

16. The Code of Practice for Official Statistics requires that "the cost burden on data suppliers should not be excessive and should be assessed relative to the benefits arising from the use of the statistics" (Principle 6).

17. We are committed to minimising the burdens associated with the production of statistics, and we will ensure that the costs of providing us with access to data are proportionate to the benefits accruing from the use of the statistics produced from these data. We will also ensure that any decisions concerning the volume or type of data we seek are informed by this commitment. We will work with data suppliers to establish data access arrangements that minimise the cost burden and potential for disproportionate impacts on taxpayers and data suppliers alike. We undertake to seek data from national or consolidated sources before placing burdens on local service providers and, where the same data can be obtained from multiple sources, to ensure that our decisions on which source(s) to access are informed by considerations of associated costs and burdens to the data suppliers.

Principle 6: Collaboration

18. We will consult with, and consider the advice of, data suppliers before issuing a notice or requesting access to data. We commit to exploring collaborative solutions and negotiated data arrangements in preference to issuing requests or notices to enable this access. This will ensure that data access arrangements are appropriately tailored to the specific needs, resources, interests and cultures of data suppliers, as well as the particular sensitivities and risks associated with different types and sources of data. A collaborative approach will also enable us to understand the way the data are constructed and therefore any caveats concerning their quality, interpretation and use. We will invoke our statutory powers of compliance and compulsion as a last resort only once all other reasonable means of accessing the data have been exhausted (including senior level discussions between the Authority and the data supplier).

Part 4: Governance

19. We will monitor the ways in which we are using the legal framework to access data by establishing an advisory data access oversight function as part of the governance structure of the Authority and drawing on the experience and independent expertise of individuals from a wide range of sectors and organisations. This function will assess data access proposals against the principles above and will provide impartial and independent advice to the National Statistician to support him/her on the exercise of his/her functions. We will publish reports and other papers detailing this advice in accordance with the Authority's general commitment to transparency.

20. We will in addition publish, consult on and maintain up-to-date supplementary guidance and best practice documents concerning the way we exercise our statutory responsibilities under this legal framework. These documents, which we may re-issue from time to time to reflect changing practices and the development of professional expertise, will provide additional clarity to help data suppliers understand their obligations and, in particular, the operational means by which we will exercise data access powers. They (will) also provide information for statistical users and the general public seeking to understand the procedural arrangements governing the way third-party data is collected, processed and safeguarded in the production of official statistics and for statistical research. These documents (will) include guidance concerning:

    - **Data requests and notices:** guidance concerning the format in which we will request data or issue notices under this legislation;
    - **Minimising burden:** the means by which we will assess the burden on data suppliers and the ways we will minimise these burdens.
    - **Data supply and transmission:** technical guidance about the format(s) for the transmission of data and safeguards to ensure data is transmitted securely;
    - **Security and confidentiality:** summary information about the ways in which we ensure the highest levels of data security and the confidential storage, processing, use and dissemination of data held in our systems; and
    - **Representation and dispute resolution:** arrangements where data suppliers can query or challenge requests for data made by us, including representations to our data access oversight function.

Code of Practice on Changes to Data Systems

Part 1: About the Code

21. This document has been prepared in accordance with the provision set out in section 45G of the Statistics and Registration Service Act 2007 that the UK Statistics Authority and its executive office, the Office for National Statistics (collectively referred to hereafter as the "Authority"), prepare, consult on and publish a code of practice on changes to data systems that may be made by public authorities who are supplying data to the Authority to support the production of official statistics and statistical research.

22. This requires public authorities to have regard to this code when considering or making changes to their data systems. The code is therefore principally intended to provide guidance for public authorities who are supplying data to the Authority for the purpose of producing statistics or conducting statistical research. However, the guidance will have practical relevance for all organisations who supply data for official statistics (or those who may be required to provide data in the future), regardless of the status of the organisation, or the frequency and means by which data is supplied.

Part 2: Understanding the power

23. The Digital Economy Bill makes a number of changes to the law governing the way data is collected for the production of statistics in the UK. The Bill amends the Statistics and Registration Service Act 2007 by, amongst other things, granting the Authority access to data held by public authorities and private undertakings in support of the Authority's statistical functions. The changes made to the Statistics and Registration Service Act 2007 by the Digital Economy Bill expand the range of data sources the Authority will be able to draw on in the production of official statistics. The data provided for this purpose may range from specific records or variables within a larger dataset – but they might be one or more entire datasets, or even metadata.

24. The precise nature of, means by which and the frequency with which data should be made available to the Authority will be set out as part of a data access agreement. In some cases the legislation also permits the Authority to

set out obligations as part of a formal agreement to provide access to data requiring data suppliers to consult with the Authority before making changes to the data they collect, the way they collect or process these data, as well as any arrangements providing the Authority with access to these data. In such cases, the access agreement will set out details of this obligation including the changes that are sufficient to trigger this obligation and the period of notice the data supplier must provide.

25. This provision is intended to support the continuity of data supply, thereby maintaining the integrity, accuracy and reliability of statistics and statistical research derived from these data – an essential safeguard if the UK statistical system is to reduce its reliance on traditional survey-based sources in favour of directly accessing administrative and other sources.

26. Where such an obligation is not set out in the agreement, the Authority nonetheless recommends that data suppliers consider whether any changes they are considering making to data systems will impact on any aspect of the data they are supplying (or may supply) to the Authority. The guidance below will help data suppliers identify the possible impacts changes to data systems may have, and to minimise the potential such changes have to disrupt the supply, or otherwise undermine the integrity of data that is critical for the production of official and National Statistics.

Part 3: The importance of consultation

27. There are a number of reasons why a data supplier may seek to change the way it collects and processes data – including to meet strategic, operational or financial challenges, as a consequence of organisational transformations or changes in staffing structures, or in response to emerging security challenges. Any guidance provided here or statutory obligation set out in a notice therefore **does not change** the right of a data supplier to make such changes in response to its own business or organisational needs. It is instead a means of ensuring that the Statistics Authority is made aware of these changes to the extent to which they impact on the nature of the data, or of the provision of that data, that it receives and relies upon for the production of statistics and statistical research.

28. There are a number of changes that may impact on the supply of data, which includes for illustrative purposes:

    - **The type of data collected, or the way the data are collected:** Changes to the nature of the data collected which are or may be passed to the Statistics Authority could have impacts on statistics that rely on these

data. Where a data supplying organisation decides to stop collecting data it provides for the production of statistics, for instance, the Statistics Authority will need to be informed in sufficient time to secure other sources to avoid disruptions to important statistical outputs that rely on these data. Similarly, changes to the way data are collected may have possible implications for the quality, reliability or usability of the data.

- **The way data are organised, stored and retrieved:** in most cases, this will have no impact on the provision of data for the production of statistics. There are some instances, however, where changes to data infrastructures may impact on some aspect of this provision, for example in how the data are transmitted to the Statistics Authority which could have the potential to interrupt the supply of data and therefore a corresponding impact on integrity of the statistics or statistical research the Authority produces. Being aware of these changes will give the Statistics Authority the opportunity to engage with the data supplier to ensure the data continue to be supplied in a safe, reliable and cost-effective way.
- **The way data are supplied:** the Authority publishes technical guidance concerning the formats it requires for transmitted data and will work with data suppliers to establish data access arrangements that minimise the costs and burdens data suppliers might accrue.

29. Being made aware of any changes a data supplier intends to make to the way it transmits data will enable the Statistics Authority to adjust its practice to ensure it continues to access the data held by data suppliers in as efficient and least burdensome way as possible.

30. Not every change to the way data is collected and processed will affect data that is being provided for statistical purposes. However, in order to identify whether this is the case or not data suppliers will need be aware of all data that is being supplied or shared, of the duration of the agreement, and the way in which that data is being shared or transmitted. As discussed above, the Statistics Authority will ensure that all these details are set out within the framework of a data access arrangement, and that any changes to the obligations of a data supplier or provision arrangements are recorded in an amendment. Data suppliers should ensure that staff responsible for considering and implementing changes to data systems are appropriately familiarised with these agreements.

31. Similarly, not every change will have a direct impact on the quality and continuity of data upon that is relied upon for the production of official statistics and statistical research. During initial data access negotiations the Authority will engage with data suppliers to ensure they understand the role supplied data will have in the production of statistics, and to therefore help the data supplier to anticipate the impact of changes it is considering to the way it collects or processes this or related data.

32. Where a data supplier does believe proposed changes may have an impact on any aspect of the official statistics that make use of the data, or on the agreed arrangements for supply, it should advise the Statistics Authority in a timely fashion. There will be some occasions when changes to data systems happen much more quickly, such as where a security vulnerability has been discovered or a business opportunity has arisen. In all such cases data suppliers should ensure they contact us **as soon as possible** once they become aware of the need to effect a change. Where a data supplier is uncertain about the impact on statistics or statistical research of changes to their data systems the Statistics Authority recommends the data supplier contact the Statistics Authority to discuss. The Statistics Authority will work with the data supplier to understand the nature of the changes and any impacts, to identify steps to maintain continuity of supply, and to ensure that supply is maintained in a way that keeps burdens to a minimum.

33. In the vast majority of cases, the data processor will itself initiate changes to the way data is collected or processed. There are, however, occasions, where a data supplier may become aware of a change that was unintended but might impact on the Authority's capacity to deploy these data in the production of official statistics or statistical research. Such changes include a change in the nature of the data being supplied, in the way it is processed, or to the infrastructures within which it is processed. Evidence of data **breaches**, **security vulnerabilities** or the **misuse of data**, for instance, will have implications for the security procedures related to the transmission, storage and use of data that have been set out in the data access arrangements. Similarly, **evidence of errors**, **inaccuracies or omissions in data**, or **fallibilities in the way the data is collected**, will have implications for the quality of the data and therefore the methodological commentary accompanying statistical outputs. Large inaccuracies or methodological flaws might even call into question the extent to which the data can be relied upon for the production of official statistics. Where such issues are identified the data supplier must advise the Authority **at the earliest opportunity**, and **in any case no later than XXX working days** after the failing is discovered.