Home Office

Draft Data Sharing Code of Practice

Code of practice for civil registration officials disclosing information under section 19AA of the Registration Service Act 1953

Presented in draft to Parliament pursuant to section 19AC(6) of the Registration Service Act 1953 for approval by resolution of each House

Contents

Part 1: About the Code of Practice

1. This Code explains how the discretionary powers contained in the Registration Service Act 1953 should be used by civil registration officials when sharing registration information with other civil registration officials and with specified public authorities for the purpose of enabling the recipient to exercise one or more of their functions. In addition, it provides civil registration officials with guidance on procedures that need to be followed when considering requests to disclose registration information. This includes details about the application process, decision-making process and governance procedures.

2. The Code should be read alongside the Information Commissioner's data sharing code of practice, as altered or replaced from time to time, which provides guidance on how to ensure personal data is shared in a way that is lawful, proportionate and compatible with data protection legislation[1]. The Code should also be read in conjunction with procedural guidance that civil 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. In this Code 'data sharing' has the same meaning as in the Information Commissioner's data sharing code of practice, 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. Examples include:
    - 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.

4. Before making disclosures under these data sharing powers, data sharing agreements will need to be put in place to outline the responsibilities of recipients of data and any necessary actions that

[1] In this Code, "the data protection legislation" means the full, applicable data protection framework as set out in the Data Protection Act 2018. This encompasses general processing (including the General Data Protection Regulation and the applied GDPR), law enforcement processing, and intelligence services processing. References to "the Data Protection Act 1998" in the Digital Economy Act 2017 are amended to "the data protection legislation" by the Data Protection Act 2018.

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 between civil registration officials and recipients of data.

5. Public authorities will need to satisfy themselves that they are complying with data protection legislation. 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 Part 6.

6. The Information Commissioner's Office has been consulted in the preparation of the Code to ensure that it is consistent with the Information Commissioner's data sharing code of practice.

The Code's status

7. The Registrar General for England and Wales has prepared and issued this Code under section 19AC of the Registration Service Act 1953[2]. It is a statutory Code which has been approved by Parliament.

8. The Code relates to civil registration in England and Wales only, as civil registration is devolved in Scotland and Northern Ireland.

9. Civil registration officials must have regard to the Code when sharing information with public authorities and other civil registration officials.

[2] The Digital Economy Act 2017 inserts new sections 19AA, 19AB and 19AC, concerning the disclosure of information by civil registration officials, into the Registration Service Act 1953.

Who should use the Code?

10. All civil registration officials with nominated responsibility[3] for disclosing information under Section 19AA of the Registration Service Act 1953 must have regard to this Code.

Specific benefits in using the Code

11. The key benefits of using the Code include:

- **Compliance with current policies and guidance**
  The Code provides civil registration officials with assurance that they are following the most appropriate policies and guidance when sharing registration information. By complying with guidance, civil 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 civil registration officials are complying with the law when sharing information. These include adherence to data protection legislation and the Human Rights Act 1998.

- **Security Provisions**
  The Code sets out how information should be held and controlled by civil registration officials. This includes details of the safeguards that should be in place for protecting information and measures to prevent information being shared where there is no legal basis for sharing information in line with the requirements of the data protection legislation. In addition, it includes policies relating to data retention, and destruction, and provisions that ensure that data is not retained for longer than is necessary.

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

[3] 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.

Part 2: Principles governing the disclosure of information

12. Civil registration officials should follow the following principles relating to the disclosure of civil registration information. These are in addition to applying the six data protection principles set out in Part 4 of this Code.

- **Principle 1: Disclosures must always be made in accordance with the requirements of data protection legislation**
  Civil registration officials must ensure they adhere to data protection legislation and have regard to any relevant codes of practice that are issued by the Information Commissioner. These include the Data Sharing Code, Privacy Impact Assessment Code and Privacy Notice Code.

- **Principle 2: Disclosures may only be made for the purpose of a public authority or civil registration official fulfilling their function(s)**
  Information must only be disclosed to enable the recipient to exercise one or more of their functions, in line with the requirements of s. 19AA(2) of the Registration Service Act 1953. Where a data applicant is unable to clearly demonstrate that information is required to meet their function, information must not be disclosed. In addition, before taking decisions as to whether personal information should be used as part of an information sharing proposal, there should be careful consideration as to whether information sharing is necessary to complete that objective.

- **Principle 3: Disclosures must not be made where there are statutory restrictions on sharing information**
  Information must not be disclosed where there are express statutory restrictions preventing disclosures of information – for example, disclosing particular information relating to adoptions and gender recognition.

- **Principle 4: Data sharing agreements should restrict the ability to create identity datasets**
  Data sharing agreements should, subject to limited exceptions[4], try to

[4] A limited exception would be for example where a dataset is held, for national security purposes, further to a warrant approved by a Judicial Commissioner under Part 7 of the

prevent public authorities from using information in a way that creates any identity datasets[5]. Data sharing agreements should include details of retention policies that prevent the linking of records in any way that could create identity datasets.

- **Principle 5: Decisions to disclose information should always be made at the right level**
  Only nominated civil registration officials should make decisions to disclose information and in doing so should ensure that disclosures are proportionate in relation to carrying out the function for which the information is required. **The Registrar General must provide written agreement prior to any large amounts of information being released (see paragraph 36).**

Investigatory Powers Act 2016.

[5] An example of an identity dataset is data consisting of a number of personal attributes on individuals such as names, previous names and other information that could be used for identification purposes.

Part 3: Understanding the civil registration powers

The gateway in the Registration Service Act 1953

13. Section 19AA of the Act provides authority for civil registration officials to disclose information[6]:
    - held in connection with any of their functions;
    - with:
        - a specified public authority[7]; 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.

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

[6] Registration information means 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.

[7] Each of the following public authorities is a "specified public authority" for the purposes of section 19AA—
(a) a Minister of the Crown;
(b)the Welsh Government;
(c) a department of the government of the United Kingdom;
(d) the Greater London Authority;
(e) a county council in England;
(f) a district council in England;
(g) a London borough council;
(h) the Common Council of the City of London in its capacity as a local authority;
(i) the Council of the Isles of Scilly;
(j) a county council in Wales;
(k) a county borough council in Wales;
(l) an NHS body within the meaning of the National Health Service Act 2006 (see section 275 of that Act).

Restrictions on this type of disclosure

15. Section 19AA does not allow for disclosure where there are express statutory restrictions on sharing information. Where there are restrictions on the sharing of particular information relating to adoptions[8] or gender recognition[9], for example, those will continue to apply and any personal data may only be disclosed subject to those restrictions. Nominated individuals or business areas with responsibility for sharing information should seek advice from policy and/or legal colleagues if they have any concerns about disclosing information where statutory restrictions might apply.

[8] See section 79(3) and 81(3) Adoption and Children Act 2002.
[9] See section 22 Gender Recognition Act 2004.

Part 4: Data sharing and the law

Data Protection Legislation

16. Disclosure under the Registration Service Act 1953 must also comply with data protection legislation and the Human Rights Act 1998.

17. This Code will help civil registration officials determine whether a particular disclosure is in line with this legislation and government policy on data sharing.

18. The Code also assists in determining information that needs to be included in data sharing agreements.

19. Data protection legislation requires personal data to be processed fairly and lawfully and for data subjects to be 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 – e.g. data solely relating to deceased individuals. Data protection legislation does not apply in these instances but it is good practice to have regard to relevant principles even when there is no statutory requirement to comply with them. However, civil registration officials will still have to ensure that any disclosure complies with the Human Rights Act 1998.

20. Civil registration officials must be able to demonstrate that they are complying with the provisions contained in the data protection legislation, including adhering to the data protection principles.

21. The Data Protection Act 1998 sets out eight basic principles which must be applied to the way personal data is collected, held or otherwise processed. These principles are largely carried over to the data protection legislation (although some are strengthened or clarified).

Data Protection Principles

22. Article 5 of the General Data Protection Regulation sets out six principles relating to the processing of personal data. Personal data shall be:
    (a) "processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");
    (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those

purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ("purpose limitation");

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation");

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality")";

In addition, controllers (known as "data controllers" in the Data Protection Act 1998) must be able to demonstrate that they are in compliance with these principles. This is known as the "accountability" principle.

23. The above principles apply to general data processing. However, please note that there are slightly different principles, as set out in the data protection legislation, which apply in respect of law enforcement data processing and intelligence services data processing which should be referred to when considering those types of processing.

24. For more detail on these six principles read the ICO's guide to data protection[10] or contact your local data protection adviser.

[10] https://ico.org.uk/for-organisations/guide-to-data-protection/

The Data Protection Act 2018

25. The Data Protection Act 2018 will replace the Data Protection Act 1998, apply the General Data Protection Regulation standards (which will take effect from 25 May 2018) and implement the Law Enforcement Directive.[11] The Data Protection Act 2018 will cover general data processing, as well as law enforcement data processing and intelligence services data processing.

26. It is important for civil registration officials to be aware of the requirements and obligations contained in the data protection legislation. Although many aspects of the regime will be familiar from the Data Protection Act 1998, there are some new requirements and processes. For example some of the changes made by the General Data Protection Regulation include:
    - Changes to some of the definitions that set the scope of data protection law. For example, the definition of "personal data" is more detailed and makes explicit provision for a wider range of personal identifiers to constitute personal data.
    - The new concept of "special categories of personal data". This includes genetic data and biometric data.
    - Additional rights for individuals - such as the right to be informed or the right to have personal data rectified or erased in specific circumstances.
    - Processing of data which falls into a 'special category' due to its sensitivity is prohibited unless certain conditions are met.
    - The Information Commissioner's powers are extended - in the most serious cases; the Commissioner can issue a maximum fine of £18 million (€20 million) or 4% of turnover. The data protection legislation ensures the Commissioner's powers to issue fines are subject to certain safeguards, including the form of notice given and a right of appeal. The data protection legislation also includes information about how to exercise appeal rights.

Controllers

27. Data protection legislation defines a controller as a person (either alone or jointly or in common with other persons) who determines the

[11] The Law Enforcement Directive (EU 2016/680) concerns the processing of personal data by competent authorities for law enforcement purposes. The Data Protection Act 2018 transposes the provisions of the Law Enforcement Directive into UK law.

purposes for which and the manner in which any personal data is processed – i.e. obtaining, recording or disclosing personal data. Controllers are responsible for ensuring the 6 principles set out above are applied to all personal data for which they are responsible. Furthermore, controllers are required to keep records of their data processing activities.

28. The controller for birth, death and marriage information, is the superintendent registrar, other than where the information is held by a registrar, in which case the registrar is the controller. In addition to registration data, registration officers may also be controllers, or joint controllers, for other personal information e.g. certificate application data. The controller for civil partnership information is the registration authority[12]. The Registrar General is a controller for information that he holds following the record being certified by the superintendent registrar.

Human Rights Act 1998

29. Civil 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 which is incompatible with rights under the European Convention on Human Rights.

30. Article 8 of the Convention, which gives everyone the right to respect for his or her private and family life, his or her home and his or her correspondence, is especially relevant to sharing personal information. Whilst sharing information relating to deceased individuals is not treated as personal data under data protection legislation, consideration should be given to whether sharing information could impinge on the right to private life for the relatives of deceased individuals, in accordance with the Human Rights Act 1998.

31. The Information Commissioner's guidance advises that if information is being shared in ways that comply with data protection legislation, it is

[12] A registration authority is defined in section 28 of the Civil Partnership Act 2004 as:
(i) a county council in England;
(ii) the council of any district in England comprised in an area for which there is no county council;
(iii) a London borough council;
(iv) the Common Council of the City of London;
(v) the Council of the Isles of Scilly;
(vi) a county council in Wales;
(vii) a county borough council in Wales.

also considered likely that the sharing would comply with the Human Rights Act 1998. Nonetheless, nominated individuals or business areas with responsibility for sharing information must ensure that disclosures are compatible with Article 8 of the Convention and should seek advice from legal advisers if they have any concerns.

Part 5: Deciding to share information under the powers

Who can share information?

32. It is important that all civil 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 civil registration official. Decision-making responsibility for sharing information will be in accordance with the General Register Office (GRO) or local authority policies and guidance. Nominated civil registration officials 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 the GRO Fraud and Disclosure Unit. 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.

33. All civil registration officials should 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 information is disclosed by a civil registration official, written agreement should be obtained from the nominated civil registration officials or business areas that have responsibility for sharing information. The written agreement should confirm that there is a legal power to share information and confirm exactly what information may be released.

Is there a legal gateway?

34. Prior to sharing information, nominated individuals or business areas with responsibility for sharing information, should be satisfied that any disclosures will be compatible with Section 19AA of the Registration Service Act 1953.

35. The permissive gateway under the Registration Service Act 1953 allows civil registration officials to share information which they hold in connection with their functions with specified public authorities or other civil registration officials to assist them to fulfil their public functions.

This is a discretionary power, with civil registration officials being able to determine whether or not it is appropriate to share civil registration information that has been requested.

When is it appropriate for data to be disclosed?

36. Sharing registration information with public authorities brings benefits to the public accessing public services and also improves the efficiency of those services. The purposes for which information can be shared using these powers includes, but is not limited to:

- **Facilitating local authority planning** – providing civil registration information to local authorities to enable them to effectively deliver public services. For instance, information on births that have occurred in one district, but which concerned those residing in a neighbouring district, could be disclosed to local authorities to allow them to more accurately plan the provision of health care, school planning and other local services.

- **Safeguarding children** – disclosing information to local authorities and NHS bodies to enable them to safeguard children within their districts. For instance, disclosing birth data to a local authority to assist social services to target engagement with one of a child's parents in the interest of that child.

- **Removing barriers when accessing government services** – providing public authorities with verification against civil registration records. For instance, disclosing birth data electronically to a public authority to remove the reliance on citizens having to provide paper certificates to access a public service.

- **Combating Housing Tenancy fraud** – disclosing registration information to local authorities in order to help combat housing tenancy fraud. For instance, disclosing death data to a county council to enable them to check whether the listed tenants of social housing are presently alive, thus preventing someone else from fraudulently living in the property when they have no right to do so.

- **Combating Blue Badge fraud** – disclosing registration

information to prevent the continued use of a Blue Badge following the death of an individual to whom it belonged. These powers allow registration officials to share death data with local authorities to help reduce the level of fraud.

- **Combating 'living together' fraud** - disclosing marriage data to public authorities in order to prevent services being delivered to individuals not entitled to the service because of their marital status – e.g. if the person is claiming benefits or services only payable to individuals who are single or lone parents.

- **Improving statistics** – disclosing civil registration information to public authorities in order to help them create statistics to improve their delivery of public services. Examples include;
  - Helping plan future resource requirements;
  - Helping develop future policies;
  - Sharing "point of contact" details within local authorities following a birth or death;
  - Sharing details on births or cause of deaths in relation to establishing public health statistics.

- **Recovering medical equipment** – disclosing information to NHS bodies or local authorities about deaths occurring within their districts in order to help them recover un-needed medical equipment following the death of an individual.

- **Sharing registration information for list cleaning purposes**- having up to date records is highly important to all public authorities and using civil registration information for 'list cleaning' purposes can help ensure records are kept up to date. List cleaning allows records that are no longer relevant to be deleted or marked as inactive. Examples of its use include:
  - Removing records relating to deceased individuals from systems;
  - Ensuring the accuracy of information held on systems;
  - Preventing correspondence being issued to the families of deceased individuals, therefore preventing unnecessary distress.

When is it not appropriate for data to be disclosed?

37. There are a number of instances where it would be inappropriate to disclose civil registration information due to either the nature of the

information or the purposes for which the information could be used. Examples of the types of disclosures not permitted using these powers include, but are not limited to:

- **Where statutory restrictions are in place** – it is not permitted to disclose information where there are statutory restrictions in place that prevent disclosures being made. For example disclosing gender recognition or adoption records where legislation prevents disclosures.

- **If it is not proportionate to disclose information** – it is not permitted to disclose excessive volumes of information or particularly sensitive data if such disclosure would be disproportionate to the intended purpose for the data. For example, it would not be appropriate to disclose data relating to a very large number of individuals when the purpose of the disclosure was to try and establish details about one individual.

- **If the data is likely to be used for non-related functions** – it is not permitted to disclose information where it appears that the recipient primarily intends to use the information for matters other than their official functions – even if the data is required for their official functions too.

- **Where there are concerns over data security** – it is not permitted to disclose information if registration officials are not satisfied with the security measures the recipient has in place to safeguard the data. Registration officials also need to be aware of any previous issues or breaches relating to a recipient's ability to maintain data securely and must not disclose information again until any issues have been resolved fully.

- **Where the information might be shared with wider organisations outside of the functions for which it was provided** – it is not permitted to disclose information for any onward sharing outside of the functions for which the information was disclosed. Registration officials will need to ensure that any onward disclosures or access to the information do not fall outside of the data sharing agreement under which the information was disclosed.

- **If the information could be used to create identity datasets** – disclosures are not permitted, apart from the limited

exceptions noted in Principle 4 at Part 2 of this Code (relating to national security), for the purpose of creating any identity datasets. For example, where it appears:

I. The applicant is intending to use the data for the purpose of creating identity datasets; or
II. There is an identifiable risk the applicant might use the data to create identity datasets.

- **If the recipient is not a listed public authority** – it is not permitted to disclose information to any public authority or other recipient that is not permitted in the legislation. Civil registration officials must always ensure that the recipient applying for information is listed in these provisions and is permitted to receive information.

How the powers should be used by registration officials

38. Only nominated registration officials have authority to disclose civil registration information under these powers. In doing so, they should be fully satisfied that all requests for information are directly related to fulfilling one or more function(s) of the recipient.

39. The application process serves the purpose of obtaining sufficient information to allow an assessment of the legal, technical and security considerations associated with the application. Registration officials, in discharging their discretion to disclose information, need to ensure that all applications provide sufficient supporting information and evidence to justify a requirement for civil registration information to meet their function. If there are any doubts about whether information is needed further information must be obtained from the applicant in all cases.

40. Registration officials with nominated responsibility for disclosing registration information should follow internal procedures for considering applications prior to any decisions being made to disclose information. These include assessing the impact of the request for information across individual business areas where relevant, both operational and policy, to seek views on the application. The purpose of doing this is to ensure that no issues are identified and that information is only disclosed where it is lawful, proportionate and compatible with data protection legislation.

41. All requests for information need to be recorded and scrutinised as part of the application consideration process. All applications should be

logged internally so as to ensure there is a full audit trail of the application, the purpose for which the information has been sought and the outcome of the decision-making process. The output of each decision-making process should result in:

- An approval – a formal notification will be issued to the applicant advising them of the decision and the next steps – e.g. completion of a data sharing agreement.
- A rejection – a formal notification will need to be issued to the applicant to inform them of the decision and any follow-up action they may want to consider – e.g. revising and re-submitting their application.
- Seek additional information – a request for more information or clarification on any issues should be sought prior to a decision being taken on whether or not to disclose information. The request will then need to be reconsidered.

Process for using the data sharing powers

43. When intending to make a disclosure under the powers in the Registration Service Act 1953 registration officials should follow the steps below:

Step 1: Identify the function for which the information is to be used and the data required to support the function

- Determine the purpose for which information is to be used by the recipient.
- Clarify any issues or queries with the applicant if there are any concerns about how information will be used.
- Request additional information if there are any uncertainties or doubts.

Step 2: Impact the proposal across any relevant business area

- Share the application with any relevant business areas prior to making any decisions to disclose information.
- Seek advice from legal advisers and data protection officers wherever necessary so as to ensure the proposal fits with the intended use of the powers and complies with data protection legislation.
- Capture and record any concerns or issues to inform the decision and outcome of the application.

Step 3: Make a decision on the application

- Determine the outcome of the application: approve, reject or seek additional information.

- Refer the application to the Registrar General for a decision to be made where relevant.
- Complete a Data Sharing Agreement and Privacy Impact Assessment.

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

42. In instances where large amounts[13] of information are requested, civil registration officials should notify the Registrar General and obtain written agreement for disclosing the information. The only exceptions are where the Registrar General has previously authorised disclosures of this type and has issued guidance permitting future disclosures. This safeguard will ensure consistency of information sharing across the civil registration service.

Criteria for sharing information

43. A primary requirement for sharing registration information with specified recipients under s19AA of the Registration Service Act 1953 is that the information to be shared is required in order to enable the recipient to fulfil one or more of their function(s).

44. In addition, civil registration officials should also consider whether:
    - the disclosure of information is compatible with the principles governing the disclosure of civil registration information contained in Part 2;
    - in their role as controller (i.e. those civil registration officials with nominated responsibility for sharing information in accordance with GRO/Local Registration Service policy), if it is appropriate and justified to take part in the arrangements - for example if there are any perceived conflicts of interest with sharing information;
    - they can meet the requirements of data protection legislation when participating in the data sharing agreement;
    - civil registration officials have the resource and technical capacity to either release information or provide responses to data-matching requests – e.g. yes/no responses;
    - the information that has been requested is adequate and not considered excessive for the purpose for which it has been requested. Only the minimum necessary information should be provided in line with the specific requirements of the recipient.

[13] For the purposes of this code, large amounts of information is defined as over 1,000 records either singly or cumulatively over a 12 month period.

45. Civil registration officials should also 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 6: Fairness and transparency

Lawful processing

46. Whilst civil registration officials have discretion to share any information they hold in connection with their own functions under section 19AA of the Registration Service Act 1953, exercise of that discretion is subject to important limitations. The disclosure of information under section 19AA of the Registration Service Act 1953 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 information must not be subject to another express legislative restriction on disclosure and the disclosure must be in accordance with data protection legislation.

Fair processing

47. When using the data sharing powers, registration officials are required to ensure that data sharing practices are fair and transparent[14]. Information should only be disclosed once the civil registration official is satisfied that all processes are fair and transparent. This is necessary to comply with the data protection legislation's "lawfulness, fairness and transparency" principle. In addition, controllers must be able to demonstrate that they have complied with the "lawfulness, fairness and transparency" principle.

48. Civil registration officials and public authorities are therefore required to have fair and transparent processes in place for disclosing and receiving information – e.g. by actively communicating how information is being used (by which bodies) via the use of a privacy notice that is provided either directly to individuals or otherwise made available to individuals.

49. Privacy notices describe all the privacy information that civil registration officials make available or provide to individuals about what civil registration officials do with their personal information. Privacy notices must be published and made available to the public in line with fairness and transparency principles as set out in the Information Commissioner's privacy notices, transparency and control code of

[14] GDPR Principle 1 states that personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals ("lawfulness, fairness and transparency").

practice[15] - which provides guidance on the content of these notices and where and when to make them publicly available.

50. Civil registration officials should also satisfy themselves that the public authorities' processes are satisfactory for the types of information which is being disclosed before any information is shared, and should discuss with the recipients what their arrangements will be. In considering whether to share information, civil registration officials should also consider what conditions need to be imposed on the future use, onward disclosure and retention of information by way of data sharing agreements. Any conditions will need to be clearly specified prior to disclosing information.

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

52. In some instances, it may be impracticable to inform individuals that their information has been shared, for example, if birth data is shared across local authority boundaries for the purpose of school planning. However, civil registration officials and public authorities will need to comply with requirements of data protection legislation to ensure that information has been shared fairly and lawfully. It will also be necessary to complete standardised records of information shared for audit purposes, detailing the circumstances, what information was shared and an explanation as to why the disclosure took place.

53. The Information Commissioner's Office has produced 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.

Data protection exemptions

54. Data protection legislation 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 provided by that legislation. Civil registration officials should consider the exemptions set out in data protection legislation and should contact nominated

[15] https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

GRO or local authority individuals with responsibility for information sharing for advice if it appears that an exemption may apply and information could not be disclosed unless it is relied upon.

Data Sharing Agreements

55. The ICO's Data Sharing Code of Practice states that it is good practice to have a data sharing agreement in place, and to review it regularly, particularly where information is to be shared on a large-scale, or on a regular basis. Civil registration officials should follow procedural guidance in developing data sharing agreements[16] required when disclosing information under these powers.

56. Prior to entering into data sharing agreements with a public authority, civil registration officials should agree with the public authority that they will take appropriate organisational, security and technical measures to:
    - Prevent, subject to limited exceptions,[17] civil registration information being linked, either with itself or with other government information, 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[18];
    - prevent accidental loss, destruction or damage of information;
    - ensure only people with a genuine business need have access to the information.

57. Public authorities will need to satisfy themselves that they are complying with data protection legislation and should be advised to seek their own legal advice regarding data sharing following any agreements to access registration information.

58. The data sharing agreements 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 information – ensuring that the recipient is

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

[17] A limited exception would be for example where a dataset is held, for national security purposes, further to a warrant approved by a Judicial Commissioner under Part 7 of the Investigatory Powers Act 2016.

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

aware that registration information is only as accurate as at the time it is captured and will be treated as such;
- precise details of what exact information is required to enable them to perform the function for which it is requested;
- restrictions on sharing certain categories of information – i.e. adoptions and gender recognition information;
- restrictions on any onward disclosure of information;
- information handling responsibilities, including details of any data processors or subcontractors;
- conditions for data processing, including whether data subjects are aware of how their information is being shared;
- 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 information;
- sanctions for failure to comply with the agreement or breaches by individual staff.

59. Data sharing agreements should contain details of sanctions that will apply to recipients of information who are found to be processing information unlawfully or inappropriately. These sanctions will include, but are not limited to:
    (a) public authorities ceasing to receive information from civil registration officials. Regulations may be made to amend the list of public authorities to whom information may be disclosed under section 19AA;
    (b) civil registration officials reporting the recipient and incident to the Information Commissioner's Office who will decide whether penalties are applicable;
    (c) civil registration officials determining whether any misconduct in 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 information again;
    (e) public authorities that have previously breached a data sharing agreement only being granted access to information again if

civil 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.

60. Both the General Register Office and Local Registration Service should maintain up-to-date lists of their individual data sharing agreements for audit purposes. Furthermore, controllers and processers will be required to maintain records of processing. These should contain a description of the categories of data subjects and the categories of personal data processed as well as the categories of recipients of such data. These records should be made available to the Information Commissioner's Office on request.

Register of information sharing activity

61. Information about all data sharing agreements under these powers should be submitted to the Government Digital Service (GDS) in the Cabinet Office who will maintain a searchable register available to the general public. The register will allow Government and the ICO to understand what data sharing is taking place under the provisions, to assess the value of the provisions as well as run audits where appropriate and to check compliance with legislation and this Code and other security and data processing guidelines.

62. Civil registration officials should submit any information required by GDS for the purpose of populating or maintaining the register.

Privacy Impact Assessments

63. Civil registration officials entering into data sharing arrangements under these data sharing powers should follow the Information Commissioner's Conducting Privacy Impact Assessments code of practice[19]. The code provides guidance on how and when to conduct privacy impact assessments at key points during the data sharing process, and how these should be amended to reflect key changes such as change in scope or circumstances. The code also includes screening questions to determine when privacy impact assessments are required and guidance on publishing privacy impact assessment reports. Civil registration officials should ensure that any sensitive information is redacted from any published reports and should also keep a record of redactions in each case and the reasons for making them.

[19] https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Part 7: Governance

Application process

64. 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 civil 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 as consistent as possible.

65. Questions that should form part of the application process include:
    - What information is being requested?
    - Why is access to information necessary?
    - For what specific purpose and public function is the information being requested?
    - How does the information being disclosed enable the recipient to perform their function(s)?
    - Are there any restrictions on what information can be disclosed?
    - What exact data items are required – e.g. names, dates of birth, gender?
    - Has the recipient of the information 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 information? Applications for disclosures amounting to 1,000 records or more over a 12-month period, either singularly or cumulatively need to be authorised by the Registrar General.
    - High-level details of security provisions that are in place/will be put in place to safeguard information 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 information and if so how will the information be deleted?
    - Is funding available to pay for costs incurred with the data share?
    - Will the data subjects be aware that their information is being shared – e.g. via a privacy notice?
    - Has a Privacy Impact Assessment been conducted/what are the findings of any such Privacy Impact Assessment?

- Are there any other benefits (including financial) of the data sharing 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's ability to deliver services is at risk
    - the Government is not able to fulfil its functions
    - impacts on citizens

66. The following key points should be understood by all those involved in the application process:
    - 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 it to fulfil one or more of their functions. Consideration will also need to be given to determine that disclosures of information are necessary and proportionate to achieve the desired objective.
    - Only minimum information should be provided to enable the recipient to carry out one or more of the recipient's functions.
    - Information sharing must be physically and/or technically possible and be compliant with data protection legislation and the Human Rights Act 1998.
    - Strict compliance with security provisions to safeguard against any misuse or loss of information, including having secure methods in place for transferring information.

Data standards and data accuracy

67. The General Register Office and Local Registration Service hold data in a number of different formats. When considering sharing information it is important that every effort is made to ensure that information is not altered or changed in any way at the point of transfer or once transferred. This will help ensure that individuals are not adversely impacted as a result of the data sharing – e.g. preventing them accessing a service where there are issues with data held by a recipient.

68. It is also important that checks are made on the accuracy of information prior to transferring information. In instances where issues arise following the transfer of information (e.g. data corruption or any other issues that impact on the accuracy of data), procedures need to be in place to allow for inaccurate information to be corrected by all

bodies holding the information. Civil registration officials should be aware of the correct procedures to follow to amend inaccurate information 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

69. The Registrar General will work with the National Panel for Registration when producing any associated guidance and on any measures to ensure that civil registration officials comply with their duty to have regard to this Code, for which he or she has responsibility.

70. 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 necessary measures to ensure the duty to have regard to the Code is complied with. In instances where data protection issues (such as data breaches) are identified, the Information Commissioner's Office will be notified at the earliest opportunity. The Registrar General will also consider notifying data subjects of any breaches[20].

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

72. The Registrar General will review the Code on an annual basis. The National Panel for Registration[21] 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.

[20] Data protection legislation will require notifications of data breaches to the ICO and potentially to data subjects themselves. This obligation would be subject to breaches being of sufficient severity to be likely to result in risk to the rights and freedoms of data subjects.

[21] The National Panel for Registration comprises local authority representatives with responsibility for delivering local registration services in England and Wales.