Data Sharing Guidance and Principles

This section of the financial framework has been significantly updated to reflect new information sharing legislation (the Digital Economy Act 2017[1]) and new data protection legislation (the General Data Protection Regulation (GDPR)[2] and Data Protection Act 2018[3]) with a view to highlighting the different sources of information that are available to local authorities. The purpose of this is to ensure local authorities are complying with their obligations under data protection legislation when working with families who are eligible for support under the Troubled Families Programme.

Part 5 of the Digital Economy Act 2017 (the DEA) consists of seven chapters. Each chapter provides the legal power for specified bodies to share information for a specific purpose. One of the provisions is a new, purpose-built legal gateway for information-sharing between specified partners who are identifying, and providing services to, households facing multiple disadvantages, including through the Troubled Families Programme. Previously, local partners had to use multiple different legal gateways for data sharing relating to different family problems, leading to complexity and to frontline staff sometimes lacking the confidence to share information. In contrast, the DEA provides a single gateway for local partners supporting families facing multiple disadvantages. Further details on this purpose built gateway – the multiple disadvantages objective – are set out below

The expectation is that this new power will be used unless there are very strong reasons for not doing so and local partnerships can expect to be challenged if they are not making use of the new power where it would be appropriate to do so. The various legacy gateways are included in this update, in recognition that this is a transition period, but these will be phased out in any future guidance.

The information in this section of the Annex is drawn from the government's Code of Practice for public authorities disclosing information under Chapters 1, 3 and 4 (Public Service Delivery, Debt and Fraud) of Part 5 of the DEA 2017[4] (referred to throughout as "the government's public service delivery code"), and the Information Commissioner's Office (ICO)'s data sharing Code of Practice[5] (referred to throughout as "the ICO's data sharing code"). Under section 43(3) of the DEA 2017, persons to whom the government's public service delivery code

[1] http://www.legislation.gov.uk/ukpga/2017/30/contents/enacted

[2] https://eur-lex.europa.eu/eli/reg/2016/679/oj

[3] http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

[4] https://www.gov.uk/government/publications/digital-economy-act-2017-part-5-codes-of-practice/code-of-practice-for-public-authorities-disclosing-information-under-chapters-1-3-and-4-public-service-delivery-debt-and-fraud-of-part-5-of-the-di

[5] https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf To note: this code has not been updated since the Data Protection Act 2018 became law and the ICO will soon publish a revised code. The draft revised code issued in September 2019 for consultation can be found here: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-data-sharing-code-of-practice/.

This section of the Annex focuses particularly on the "multiple disadvantages" objective of the public service delivery power, which is the most significant for the Troubled Families Programme.

Please note: this Annex is designed to assist agencies in making use of the information sharing powers within the DEA 2017. It does not purport to give legal advice, should not be relied on as an authoritative statement of the law and it is not a substitute for obtaining your own specialist advice, including legal advice. All agencies should pay attention to the full legislation and relevant codes of practice, which offer more information, including a step by step guide and checklist on how to use the new powers (see section 2.5 of the government's public service delivery code).

The DEA 2017

Part 5 of the DEA 2017 introduces new powers for government to share personal information across organisational boundaries to improve the delivery of certain public services. This is in recognition that public service delivery is changing, and that there is increasing acknowledgement that services are more efficient and effective when they are joined up. Joining up services requires the sharing of information.

"Information sharing" as defined in the government's public service delivery code the DEA means: the disclosure of information from one or more organisations to a third-party organisation or organisations. There is no formal definition of data sharing within the data protection legislation, although the scope of the ICO's data sharing code is defined by section 121 of the Data Protection Act 2018 as 'the disclosure of personal data by transmission, dissemination or otherwise making it available'.

As outlined above, Part 5 of the DEA 2017 covers seven chapters which provide for legal powers designed to improve the sharing of publicly held information for specific purposes. The provisions in Part 5 of the DEA 2017 were designed to enable data to be shared more easily so that public authorities can deliver their responsibilities more effectively - from better development of policy to more efficient and better targeted delivery of services.

The general public service delivery power in section 35, Chapter One of Part 5 of the DEA 2017 allows specified persons to share personal information for specified objectives which are set out in legislation. This power is aimed at supporting the improvement or targeting of public services or the facilitation of benefits to individuals or households in order to improve their well-being. Objectives for sharing under the public service delivery power must meet criteria set out in Section 35 of the DEA 2017, which reflect these purposes.

One of the objectives already established under the public service delivery power is the "multiple disadvantages" objective set out in paragraph 2 to the Schedule within the Digital Government (Disclosure of Information) Regulations 2018[6] of: ***identifying individuals or households who face multiple disadvantages and enabling the improvement or targeting of public services to such individuals or households***

[6] https://www.legislation.gov.uk/ukdsi/2018/9780111169445/contents

and providing for the monitoring and evaluation of programmes and initiatives. This objective is key to delivering the Troubled Families Programme as it provides a single gateway to share information on multiple issues, across a range of agencies.

As set out in paragraph 2 of the Schedule to the Digital Government (Disclosure of Information) Regulations 2018 (the Regulations), "multiple disadvantages" means the presence of two or more of the following factors[7], which adversely affect an individual or one or more individuals in a household:

- anti-social behaviour
- being a care leaver
- being a child in need
- criminal offending
- domestic violence
- financial exclusion
- having a disability
- homelessness
- ill-health
- irregular attendance at school
- not being in education or training
- substance misuse
- unemployment

Organisations permitted to disclose data under one or more of the information sharing powers within Part 5 of the DEA are referred to as specified persons. Some specified persons can share under more than one power and/or more than one public service delivery objective. Schedules in the DEA set out which bodies can share information under the public service delivery, debt and fraud powers. In the case of the public service delivery power, specified persons from Schedule 4 of the DEA must be assigned to the objective. This is set out in the Regulations, which created the existing 4 Public Service Delivery objectives[8].

It means that certain specified persons may be able to share information under only one of the existing public service delivery objectives whereas others can share information under more than one. In the case of the multiple disadvantages objective, the vast majority of specified persons for the public service delivery power schedule are permitted to disclose and receive information. The specified persons reference register – which sits alongside the register of information sharing agreements made under chapters 1-4 of Part 5 of the DEA - sets out each of the specified persons for the public service delivery, civil registration, debt and fraud powers within Part 5 DEA 2017, and outlines which specific powers and public service delivery objectives each of them are permitted to share information under.

Be aware that, normally, information disclosed under the public service delivery power can only be used for the purposes for which it was disclosed. However, there

[7] The factors are further defined in the Schedule.

[8] https://www.legislation.gov.uk/ukdsi/2018/9780111169445/contents

are limited instances where such information can be used by a public authority for another purpose. These circumstances vary but may include[9]:

- if the information has already been lawfully placed into the public domain;
- if the data subject (the individual to whom the personal data relates) has consented to the information being used for the other purpose;
- for the prevention or detection of crime or the prevention of anti-social behaviour;
- for the purposes of a criminal investigation;
- for the purposes of legal proceedings;
- for the purposes of preventing serious physical harm to a person or loss of human life;
- the purposes of safeguarding vulnerable adults or children;
- the purpose of responding to an emergency; or
- for the purposes of protecting national security.

A different regime applies to personal information disclosed by HM Revenue and Customs, which would include information disclosed by the Valuation Office Agency. Personal information disclosed by the Revenue and Customs can only be used for purposes other than the purpose for which it was originally disclosed with the Revenue and Customs' consent (also see below under "data protection legislation").

Documentation

Responsibility for the Public Sector Delivery data sharing powers under Part 5 of the Digital Economy Act 2017 transferred to the Cabinet Office with effect from 1 August 2020. The Code of Practice will be updated to reflect the transfer in due course. In the meantime, section 5.2 of the Code of Practice offers further information on the documentation that may be needed to accompany data sharing under the public service delivery power, including an information-sharing agreement, which should be drawn up according to the ICO's data sharing code, a data protection impact assessment and a business case. Information about all information sharing agreements concerning England-only or non-devolved bodies for a disclosure or group of disclosures under the public service delivery power must be submitted to the public service delivery secretariat. The secretariat will maintain searchable electronic registers available to the general public. Section 5.1 of the government's public service delivery code sets out further details on what information should be submitted and when redactions may be appropriate. More detailed information on how to submit, including a suggested template to follow, is available on gov.uk[10].

You must undertake a data protection impact assessment (DPIA) if you wish to share data under the public service delivery power. The data protection legislation requires DPIAs to be conducted prior to the processing of personal data when the processing is likely to result in a high risk to the rights and freedoms of individuals. The ICO's guidance on DPIAs provides further information, explaining

[9] These are set out in full in section 40 of the DEA 2017.

[10] https://www.gov.uk/government/publications/digital-economy-act-2017-part-5-codes-of-practice/guidance-for-controllers-relating-to-the-register-of-information-sharing-agreements-under-part-5-of-the-digital-economy-act

their role in demonstrating your accountability. The guidance tells you how to conduct a DPIA and includes checklists to assist the process. [11]. The DPIA should be reviewed regularly, and you may need to repeat it if there is a substantial change to the nature, scope, context or purposes of your processing.
The Information Commissioner's Office website includes a helpful guide to Data Protection Impact Assessments, a DPIA Template, and useful information about what must be included in a DPIA and other information, such as the lawful basis for the relevant processing (explained below), which the ICO recommends for inclusion.[12]

Privacy information must also be provided to individuals at the time of collecting their personal data. It should explain, among other matters, what you do with their personal information, who you are sharing it with, your retention periods for that personal data, and individuals' rights in relation to that data, such as the right to access the data or to require that it be rectified (as explained within the section entitled 'Data Protection Legislation' below). In exercising these powers to share data, you must ensure that suitably worded privacy information is published and made available to individuals in line with the fairness and transparency principles as explained in the ICO's guidance[13] and in the ICO's data sharing code. The data protection legislation now requires privacy information to be more specific and detailed than under the Data Protection Act 1998. Please see the guide to providing privacy information[14] and the right to be informed for more information.[15]

The data protection legislation[16]

While the DEA 2017 provides a legislative gateway to share information, public authorities will also need to have robust safeguards in place to ensure that people's information[17] is processed in a secure and appropriate way in line with the requirements of the data protection legislation, including the General Data Protection Regulation and the Data Protection Act 2018. It is of vital importance that data is handled in a way that inspires the trust and confidence of citizens. Section 1.2 of the government's public service delivery code sets out ten principles that support the security of data and privacy of citizens whilst enabling the delivery of better services

---

[11] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ and https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

[12] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

[13] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

[14] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-privacy-information-should-we-provide/

[15] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

[16] This 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.

[17] To note that personal information" in the DEA 2017 has a slightly different meaning to "personal data" in the data protection legislation. Both definitions need to be applied when using these powers because the requirements for "personal information" under the DEA 2017 and the requirements for "personal data" under the data protection legislation must both be observed and complied with.

and outcomes for citizens and government. All persons using the public service delivery power are required to apply these principles when they do so. These reflect, but are separate to, the Data Protection Principles set out in Article 5 of the GDPR and mentioned below, which should also be adhered to. The principles in section 1.2 of the public service delivery code are underpinned by four key requirements. In summary, these are:

- to carefully assess whether disclosure is consistent with the DEA 2017 and the data protection legislation before using the powers, and have regard to the relevant codes of practice issued by the ICO
- only share the minimum data required to fulfil the stated purpose for sharing
- have information sharing agreements that ensure that: a) where datasets are linked, subject to limited exceptions, it should be for the specified purpose and should not lead to the creation of new identity registers, and b) including details of retention and destruction policies
- to be transparent about use of the powers so citizens can understand what data is being shared, the bodies that are disclosing or receiving data, and why, again having regard to the ICO's codes of practice (see above on DPIAs and privacy information)

The data protection legislation 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 (the "lawfulness, fairness and transparency" principle). Public authorities will need to demonstrate that they are complying with the provisions contained in the data protection legislation, including adhering to the Data Protection Principles, which are listed in Article 5 of the General Data Protection Regulation and in paragraph 23 of the government's public service delivery code. In addition, controllers must be able to demonstrate that they are in compliance with these principles. This is known as the "accountability" principle. These GDPR Data Protection principles apply to data processing in general. Slightly different principles govern law enforcement data processing and intelligence services data processing. Reference should be made to the data protection legislation and specialist advice may be needed where this is relevant.

In order to process personal data lawfully and meet the "lawfulness, fairness and transparency" Data Protection Principle referred to above, at least one of the lawful bases for processing set out in Article 6 of the GDPR must apply. It is necessary to determine what the lawful basis for processing is before processing of personal data begins.

The lawful bases for processing are set out in Article 6(1) of the GDPR. The six lawful bases are known in brief as "consent", "contract", "legal obligation", "vital interests", "public tasks" and "legitimate interests".

You should consider which lawful basis best fits the specific purposes and the context of the processing you intend to carry out. In particular, certain lawful bases for processing may not be appropriate for public authorities to use. For example public authorities are not permitted to use the "legitimate interests" basis. Public

authorities should also be aware that, given the perceived imbalance of power between the public authority and data subject, relying on the data subject's consent as a lawful basis for the processing of personal data could raise questions around whether the consent was freely given and consequently whether it is valid, and that if the data subject withdraws that consent, it will not be possible to switch to a different lawful basis to continue the processing. In the context of processing data to address multiple advantages and support the Troubled Families Programme, public authorities are likely to use the "public task" basis set out at Article 6(1)(e) GDPR as it can apply to either carrying out a specific task in the public interest laid down by law or exercising official authority which is laid down by law.

Further requirements are set out in data protection legislation for the processing of special categories of personal data, including data concerning health, and for data relating to criminal convictions and offences. Organisations should consult the data protection legislation and take their own independent legal advice about the application of these provisions to their involvement with the Troubled Families programme. Further information concerning these lawful bases for processing personal data is available on the website of the Information Commissioner's Office.[18]

Public authorities are expected to be transparent wherever possible about how they are sharing data by ensuring that individuals are fully informed about how their information is being used. Public authorities must also follow the requirements on data standards, data security, and data retention and disposal as set out in paragraphs 44-53 of the government's public service delivery code, and in the ICO's guidance, including that on the principles of storage limitation and security. The GDPR requires you to process personal data "using appropriate technical or organisational measures"[19]

Individuals retain rights in relation to their personal data under the data protection legislation once it has been obtained by a third party organisation, such as a public authority. These include the following rights:

- The right to receive certain information from the organisation which controls the processing of the individual's personal data (the "data controller") about the processing and the individual's rights;
- The right to access personal data and information about the processing, for instance through a "subject access request";
- The right to require the data controller to rectify any personal data which proves to be inaccurate;

[18] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

[19] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/ and https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

- Rights to object to the processing of personal data, restrict that processing or require the data controller to erase it in certain circumstances;
- The right to receive the personal data, or require transmission to another data controller where technically feasible; and
- The right not to be subject to automated decision-making in certain circumstances.

In particular, care should be taken whenever automated processes are used to make a decision. Subject to certain exceptions, Article 22 of the GDPR prohibits automated decision-making, including profiling, which has a legal or similarly significant effect on data subjects. In this context, "profiling" refers to automated processing of personal data to evaluate certain things about an individual, such as analysing or predicting their economic situation or health.

These provisions limit the circumstances in which such decision-making and profiling can take place, and require the relevant data controller to take measures to safeguard the rights and interests of the individuals subject to such processing. The relevant safeguards include making it possible for the individuals concerned to obtain an explanation of a decision made on a purely automated basis, seek human intervention and challenge it. Data controllers engaged in such processing may also need to notify the individuals concerned of this automated processing and provide information about its logic and consequences. There are further restrictions and safeguards when such decision-making or profiling involves special category personal data, such as health data. This prohibition applies where the decision being taken is made solely by automated means. The prohibition will not apply where there is some active human involvement in the decision-making process.

Whilst automated processes are a valuable tool to increase effectiveness and efficiency, it is important to consider whether these processes lead to solely automated decisions and, if so, how to remedy this so that the decision is compliant with the prohibition under Article 22. Further details about this and these other rights listed above, the circumstances in which they do and do not apply to the processing of personal data, and how they are exercised are available on the website of the Information Commissioner's Office.[20]

Public authorities must always ensure that data sharing is compliant with the Human Rights Act 1998 (HRA) and must not act in a way that would be incompatible with rights under the European Convention on Human Rights. Article 8 of the Convention, which gives everyone the right to respect for their private and family life, home and correspondence, is especially relevant to sharing personal information. If you disclose or share personal data only in ways that comply with the data protection legislation, the sharing or disclosure of that information is also likely to comply with the HRA. You should seek specialist advice if you have any concerns about human rights issues including issues separate from the data protection elements of Article 8) regarding the disclosure or data sharing arrangement you are proposing.

[20] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Whilst sharing data relating to deceased individuals is not personal data under the data protection legislation as outlined above, you should consider whether sharing this information could affect the right to private life of the relatives of deceased individuals.

Organisations involved in the sharing of health data for the identification of troubled families may well take part in these forms of data processing. Such organisations should take their own legal advice to ensure that they are complying with data protection legislation in this respect. Further information about the rights of data subjects in these circumstances is provided on the website of the Information Commissioner.[21]

The DEA 2017 does not authorise disclosure which is prohibited under Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016, or Part 1 of the Regulation of Investigatory Powers Act 2000 its repeal by paragraphs 45 and 54 of Schedule 10 to the Investigatory Powers Act 2016 is fully in force

Legacy Legal Gateways

The following outlines the legacy legal gateways you can still consider using to share data at the time of writing. The DEA 2017 is available under all headlines, as it is a single gateway for sharing information on multiple issues across a range of agencies[22]. As set out above, the expectation is that this new power will be used going forward unless there are very strong reasons for not doing so.

As with the powers available under the DEA 2017, it is for public authorities to interpret the relevant legislation and to satisfy themselves that the use of the powers listed below is appropriate in the particular circumstances.

Gateway	Provision
Crime and Disorder Act 1998	Section 115(1)
Crime and Disorder Act 1998	Section 17A
Offender Management Act 2007	Section 14

Gateway	**Provision**
Education (Information about Individual Pupils) (England) Regulations 2013/2094	Regulations 3 and 4, S.I. 2013/2094

[21] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

[22] It is worth noting that section 35 of the DEA 2017 is not available for data-sharing with health and adult social care bodies, as these are not specified persons for the purposes of section 35.

School Discipline (Pupil Exclusions and Reviews) (England) Regulations 2012/1033	Part 4 [regulation 23]

There are a small number of children who are considered 'missing' because they are not on the school roll. These children are likely to be among the most vulnerable category of children and therefore it is important that the Troubled Families Programme identifies them as far as possible. However, it is not our intention to identify children who are being appropriately home schooled, as these children will be receiving an education from their parents.

Gateway	**Provision**
Childcare Act 2006 and the Childcare (Provision of Information About Young Children) (England) Regulations 2009 (S.I. 2009/1554)	Section 99 and S.I. 2009/1554
Childcare Act 2006	Section 13A
Children Act 1989	Section 17 (with Schedule 2, part 1)
Children Act 2004	Section 10

Gateway	**Provision**
Welfare Reform Act 2012 and the Social Security (Information-sharing in relation to Welfare Services etc.) Regulations 2012 (S.I. 2012/1483)	Section 131 and S.I. 2012/1483
Education and Skills Act 2008	Section 70
Localism Act 2011	Section 1
Education Act 1996 and the Education (Individual Pupil Information) (Prescribed Persons) (England) Regulations 2009 (S.I. 2009/1563)	Section 537A(6) and S.I. 2009/1563 regulation 3

Gateway	Provision
Crime and Disorder Act 1998	Section 115
Domestic Violence, Crime and Victims Act 2004	Section 54

Living well, improving physical and mental health and well-being: parents and children with a range of health needs

The sharing of health data for the identification of troubled families remains one of the biggest challenges for the Troubled Families Programme. Given the particular sensitivities around the sharing of personal health data, the national Troubled Families Team worked with Public Health England, Department of Health and NHS England to agree an approach that allows families to be identified for support under the expanded programme on the basis of their health needs.

The agreed interim guidance[23] recommends that a list of families that have already been identified as meeting one of the programme's indicators is shared with relevant health partners so that they can use this to flag whether any of the suggested health indicators are met. Local authorities will need to talk to relevant health partners and / or governing bodies to work out the best ways of gathering and sharing this data locally. Some local authorities may already be receiving health data or have negotiated alternative data sharing arrangements with local health partners.

As discussed above, in this context and whenever referring individuals or families for the purposes of the Troubled Families Programme, it is also important to consider the prohibition on automated decision-making at Article 22 of the GDPR.

Referrals

This Financial Framework suggests a range of indicators that can be used to identify families under the six headline problems. However, we recognise that referrals will be one important way through which local authorities can identify the families with the breadth of problems that mean they would benefit from this programme. This is why there are suggested indicators under each of the headline problems referring to 'problems of equivalent concern'.

These indicators enable referrals from professionals locally and, depending on the nature of the risk and seriousness of the circumstances, may be undertaken with or without the individual's consent. In some cases, particularly where required by one of the legacy legal gateways listed above, consent must be obtained by law before a referral is made. In cases where consent is not prescribed by law, individuals should be made aware that their data is being shared and their consent should be sought wherever possible. However, this will be a matter for local assessment and professional judgment in the circumstances of each case.

[23] https://www.gov.uk/government/publications/troubled-families-supporting-health-needs.

Given the scale of the programme, referral arrangements are unlikely to be sufficient to identify the required volumes of families in each local authority. However, the programme provides the flexibility to identify families through these means, where appropriate and as a supplement to other sources of identification