

Data sharing: Identity verification services

Consultation on draft Digital Government (Disclosure of Information) (Identity Verification Services) Regulations 2023

This consultation begins on 4 January 2023
This consultation ends on 1 March 2023

[back of cover – please leave this page blank]

Data sharing: identity verification services

Consultation on draft Digital
Government (Disclosure of
Information)(Identity Verification
Services) Regulations 2023.

A consultation produced by the Cabinet Office, also available on-line at gov.uk.

About this consultation

To:

The organisations affected by this consultation are public authorities in England, Scotland, Wales, Northern Ireland and/or other government departments, arm's length bodies, non-departmental public bodies or other organisations who may consider they could be affected by the draft regulations. It may also be relevant to other bodies that have an interest in identity verification services. The specified organisations are not meant to be exhaustive or exclusive. Responses are welcome from anyone with an interest in or views on the subject covered by this consultation.

Duration: From 4 January 2023 to 1 March 2023

Enquiries (including requests for the paper in an alternative format) to:

The Data Sharing Legislation Team at dea-data-sharing@digital.cabinet-office.gov.uk

How to respond:

We have provided a list of suggested questions for you to use when responding to this consultation in the 'Questionnaire' section. Our preference would be for you to <u>respond through our online survey.</u>

We cannot accept postal responses to this consultation unless there are exceptional circumstances. If you need to send in a postal submission please contact the Data Sharing Legislation Team to discuss options. You may correspond using the following email address

<u>dea-data-sharing@digital.cabinet-office.gov.uk</u> or, alternatively contact 07584 342684 to discuss options.

Additional activity will be organised by the Government Digital Service for bodies with an interest in how the powers will be used. More information on this activity will be provided to selected organisations in due course.

Please indicate in your response whether you are content for your comments to be published, with or without attributing it to you or your organisation.

Additional way to feed in your views:

Please send your response by 1 March 2023 to

The Data Sharing Legislation Team at dea-data-sharing@digital.cabinet-office.gov.uk

Please include the following in the subject line if you choose to respond this way: 'Response to the consultation on the data sharing for identity verification services'.

You may wish to refer to the Questionnaire section where you will find a list of the consultation questions.

Response paper:

A response to this consultation exercise is due to be published by 24 May 2023 on GOV.UK

Contents

About this consultation	2
Contents	5
Ministerial Foreword by Alex Burghart MP, Parliamentary Secretary for the Cabinet Office	7
Executive summary	10
Introduction	10
The proposal	12
What is the new data sharing objective?	12
Who will use the data sharing power?	14
Who are the new public authorities?	14
New public authorities to be added to Schedule 4 of the Digital Economy Act	
2017	15
Who may process data and why?	17
What data will be processed?	17
How will the data be shared?	18
What is the likely impact of the new data sharing power?	19
Case Studies for identity verification services	20
Why introduce the power now?	23
What other options have been considered?	24
How does the data sharing align with UK government priorities?	24
Why is the UK Government taking this proposal forward?	25
Does the data sharing power apply across England, Scotland, Wales and Northern Ireland?	25
Will data sharing comply with the relevant data protection requirements?	25
Has GDS carried out a data protection impact assessment?	26
Does the proposed data sharing comply with current best practice?	26
Why consult?	26
Impact Assessments	27
Questionnaire	28
Timetable	32
Provisional timetable for the parliamentary process	32
Contact details and how to respond	33
Annex 1 - Draft Digital Government (Disclosure of Information)(Identity Verification Services) Regulations - see separate document	34

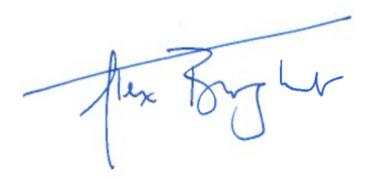
Annex 2 - Background to identity verification services	35
Annex 3 - Background to the Digital Economy Act 2017	37
What is the Digital Economy Act 2017?	37
Why and how did we develop the legislation?	37
What do the public service delivery powers do?	37
What does the Public Service Delivery Review Board do?	38
Does the Digital Economy Act 2017 align with data protection legislation?	38
Who uses the Digital Economy Act 2017?	38
Is the government committed to being open and transparent about data shared under the Digital Economy Act 2017?	1 38
Annex 4 - public authorities who would be able to share data for the purpose of the proposed identity verification services objective	es 39
Annex 5 - Privacy Notice	42
Your data	42
Your rights	45
International transfers	45
Contact details	45
Complaints	46

Ministerial Foreword by Alex Burghart MP, Parliamentary Secretary for the Cabinet Office



- This Government has made a commitment to improve the way that data and
 information is shared and used across the public sector to deliver better,
 joined up services and exceptional outcomes for our citizens. People often
 access government services in times of great need, and services must
 provide the best possible experience for users, while maintaining privacy, trust
 and building confidence.
- 2. The Digital Economy Act was designed and passed in 2017 to give us flexibility to introduce new data sharing gateways to support the delivery of key services, as the need arises, by secondary legislation and with a pre-consultation stage. This consultation sets out proposed data sharing legislation that would make it easier for citizens to prove who they are online when accessing government services.
- 3. The proposed legislation will also unlock the full benefits of a new government identity verification system, known as GOV.UK One Login. As part of the

- Cabinet Office, the Government Digital Service (GDS) is developing GOV.UK One Login, through close collaboration with other government departments.
- 4. Inclusion is at the heart of GOV.UK One Login. The proposed data-sharing legislation will ensure that more people than ever before will be able to prove their identity online and access government services, so that anybody who wants to use online services is able to. Furthermore, the government is committed to realising the benefits of digital identity technologies without creating ID cards.
- 5. GOV.UK One Login and the proposed legislation will ensure the government continues to drive inclusive digital transformation, to level up opportunities across all corners of the UK, and deliver brilliant public services. To drive this inclusive digital transformation even further, this Government is separately legislating to enable the use of trusted digital identities in the UK under Part 2 of the Data Protection and Digital Information Bill. This policy initiative is owned by DCMS and will enable citizens to prove things about themselves in a secure and trusted way to access commercial products and services online. DCMS is doing this in a way that maintains people's choice, security and control of their data, and supports growth and technical innovation across the economy.
- 6. I welcome responses from anyone with an interest or views on identity verification services to respond to this consultation.



Alex Burghart MP, Parliamentary Secretary for the Cabinet Office.

Executive summary

7. This consultation sets out the Cabinet Office's proposal to enable data sharing between specified public authorities to support delivery of identity verification services to individuals and households.

Introduction

- 8. The Public Service Delivery ('PSD') power (Chapter 1 of Part 5 of the Digital Economy Act 2017) allows specified public authorities to share personal information for objectives which are set out in regulations. This information sharing power is aimed at improving or targeting public services to individuals or households in order to improve their well-being. It also includes safeguards to make sure that the privacy of citizens' data is protected when shared by public authorities.
- New objectives can be created providing they meet the criteria in <u>Section 35</u>
 of the Digital Economy Act 2017 and secure parliamentary approval. The
 criteria are as follows:
 - condition 1: the purpose is 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;
 - condition 2: the purpose is the improvement of the well-being of individuals or households; and
 - condition 3: the purpose is the supporting of the delivery of a specified person's functions, or the administration, monitoring or enforcement of a specified person's functions
- 10. In order to exercise the PSD power, the government must, via regulations, set specific objectives for which data may be shared and identify the specific public authorities to which they apply. The Code of Practice1 for the PSD power provides the principles and guidance on using the power and on ensuring compliance with data protection legislation.

¹https://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

- 11. This consultation paper sets out:
 - a proposed objective to support identity verification services and the draft Digital Government (Disclosure of Information)(Identity Verification Services) Regulations 2023 which would enact it;
 - a proposal for 4 new public authorities to be added to the schedule of authorities able to use objectives under the public service delivery data sharing powers, subject to this public consultation and parliamentary approval;
 - a proposal for those 4 new specified public authorities to be able to use the new objective to support identity verification services specifically; and,
 - a proposed list of public authorities already in Schedule 4 of the Digital Economy Act 2017 to be able to use the new objective to support verification services specifically.
- 12. This consultation is aimed at the general public, UK public authorities and other government departments, arm's length bodies, non-departmental public bodies or other organisations who may consider they could be affected by the draft regulations. It may also be relevant to other bodies that have an interest in identity verification services.
- 13. Government has completed a number of impact assessments against the proposed secondary legislation to ensure that all intended and unintended effects have been considered and mitigations established where appropriate. We have published a summary of the Public Sector Equality Duty assessment with this consultation.
- 14. Responses are welcome from anyone with an interest in or views on the subject covered by this consultation.

The proposal

- 15. The Government Digital Service (GDS), part of the Cabinet Office, is developing, in collaboration with other government departments, a digital identity verification service which will allow people to create and reuse digital identities to access public services. Known as GOV.UK One Login, this will make it easier for people to find and access government services, allows users to prove their identity online, protects the privacy of users and reduces identity fraud and theft. The proposed legislation will allow more people than ever before to successfully prove their identity online and access government services.
- 16. In order to successfully deliver this service, participating public authorities will need to be able to check and share several types of government-held personal data with the identity verification service to allow users to prove they are who they say they are.
- 17. To support identity verification services, the UK Government is proposing to create a new objective under <u>Chapter 1 of Part 5 of the Digital Economy Act 2017.</u>² The proposed objective will enable data sharing by specified public authorities currently included in <u>Schedule 4</u>³ of the Act to deliver digital identity verification services to citizens. The proposal also includes 4 new public bodies to be added to Schedule 4 and for them to be able to share data for the purposes of identity verification services.
- 18. As required by the Code of Practice, the proposed new objective has been approved by the <u>Public Service Delivery Review Board</u>⁴.

What is the new data sharing objective?

- 19. The Digital Government (Disclosure of Information)(Identity Verification Services) Regulations 2023 will create a new PSD objective to allow sharing personal information in order to deliver identity verification services to individuals and households. It would enable data sharing between the public authorities specified in Annex 4 of this consultation. The data sharing would provide those specified public authorities with the ability to share data for the purposes of identity verification for the benefit of individuals and households.
- 20. The data sharing objective would enable public bodies to share a wider range

² https://www.legislation.gov.uk/ukpga/2017/30/part/5/chapter/1/enacted

⁴ https://www.gov.uk/government/groups/digital-economy-act-public-service-delivery-review-board

of specified data than is currently possible. This benefits individuals and households by improving digital inclusion, reducing the burden on individuals of providing the same information to different public authorities many times, and makes access to services easier.

Question 1 - The first condition for new objectives under section 35 of the Digital Economy Act 2017 is that the data sharing should either;

- a) improve or target a public service provided to individuals or households; or
- b) provide a benefit (whether financial or otherwise) to individuals or households.

To what extent do you agree that the proposed new objective meets at least one of those parts of the first condition?

Please choose one of the following options:

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree
- Don't know

Please provide the reason for your response.

Question 2 - The second condition is that data sharing should improve the well-being of individuals or households.

To what extent do you agree that the proposed new objective meets this second condition?

Please choose one of the following options:

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree
- Don't know

Please provide the reason for your response.

Question 3 - The third condition is that the data sharing should support the

delivery, administration, monitoring or enforcement of a service provided by a particular public authority (or authorities).

To what extent do you agree that the proposed new objective meets this third condition?

Please choose one of the following options:

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree
- Don't know

Please provide the reason for your response.

Who will use the data sharing power?

- 21. The public authorities who would be able to exercise the power for the purposes of the new identity verification services objective are included in Schedule 45 to the Digital Economy Act 2017 and listed in Annex 4 of this consultation. The public authorities are included because either:
 - they, or their agencies, hold data that will be used to improve the online verification of a user's identity when a user is seeking access to a government service and/or require access to the results of an identity verification check previously performed on a user; or
 - they are public authorities which are likely to be service providers rather than data providers, i.e. they will offer the identity verification service to access their services but will not be providing the source data for the definitive checks.

Who are the new public authorities?

22. Government is also consulting on adding 4 new public authorities to Schedule 4 for the purposes of the proposed identity verification services objective. Similarly, these 4 new public authorities will either hold data to verify an individual's identity and/or help to deliver the identity verification service. The

⁵ https://www.legislation.gov.uk/ukpga/2017/30/schedule/4/enacted

4 new public authorities are set out in the table below, together with the reason for including them, and also in Annex 4.

New public authorities to be added to Schedule 4 of the Digital Economy Act 2017

Public authority	Reason for including
The Cabinet Office	The Cabinet Office will provide government identity verification services to individuals, households and participating government departments.
Department for Transport	The sponsoring department for the Driver and Vehicle Licensing Agency, an executive agency which holds driving licence data.
Department for Food, Environment and Rural Affairs (DEFRA)	DEFRA manages a number of services which will offer the identity verification service to individuals so they may access their services.
The Disclosure and Barring Service (DBS)	An executive non-departmental public body, sponsored by the Home Office which holds and administers personal data necessary to help employers make safer recruitment decisions.

23. Adding new public authorities to be able to use the data sharing powers will also mean that they will be able to share data for other public service delivery objectives specified in Part 5, Chapter 1 of the Digital Economy Act 2017, subject to public consultation and parliamentary approval in each case.

Question 4 - To what extent do you agree that the following government departments should become a public body eligible to share data for public service delivery objectives (these public authorities are listed in Schedule 4)?

- Cabinet Office
- Department for Transport
- Department for Food, Environment and Rural Affairs
- Disclosure and Barring Service

Please choose one of the following options:

Strongly agree

- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree
- Don't know

Please provide the reason for your response and specify which public body you are providing views on.

Question 5 - To what extent do you agree that the following government departments should be able to share data for the identity verification objective?

- Cabinet Office
- Department for Transport
- Department for Food, Environment and Rural Affairs
- Disclosure and Barring Service

Please choose one of the following options:

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree
- Don't know

Please provide the reason for your response and specify which public body you are providing views on

Question 6 - Are there any other public authorities not proposed in this consultation which you think should be able to share data for the identity verification objective?

Please choose one of the following options:

- Yes
- No

Please provide the reason for your response.

Who may process data and why?

- 24. Only the public authorities shown in Annex 4 may process data to support identity verification services under the proposed power. The public authorities listed in Annex 4 hold personal data about individuals in the course of their normal operations. This includes organisations which hold documents which are typically used in identity verification, such as the Home Office holding passport information, and organisations holding information which can be used to support identity verification, such as HMRC holding personal data for tax purposes. Alternatively, some of the public authorities listed may deliver the identity verification service, for example the Cabinet Office, and will therefore need to process personal data.
- 25. Health and adult social care bodies are not currently included in the scope of the Digital Economy Act 2017 for data sharing purposes.

What data will be processed?

- 26. Public authorities will process the minimum number of data items, known as attributes, necessary for verifying the identity of an individual. Examples of attributes include:
 - o user's full name:
 - o date of birth;
 - home address;
 - email address:
 - photographic images;
 - various identifiers such as passport number or driving licence number;
 - attributes held by government departments necessary for verifying the identity of an individual;
 - the outcome of identity checks previously performed on a user; and
 - o transactional data, for example, income
- 27. Other data items may be processed as identity verification services develop. This may include special category data and processing will only take place in line with the relevant guidance (see paragraph below). However, any additional information to be shared will comply with the 'data minimisation' principles so that only the minimum amount of data is disclosed as is necessary for any identity check. At this time the service will not be aimed at children under the age of 13.

28. Special consideration will also be given to the handling of all personal data belonging to individuals who cannot consent to the service for whatever reason and may have a third party acting on their behalf.

How will the data be shared?

- 29. Different government services have unique identity verification criteria depending on the level of confidence required in an identity. An individual using the identity verification service to access a government service would present data to be validated against data already held by specified public authorities. This should confirm that the information submitted by the individual matches that information held by a public authority and increases the confidence that the individual is the claimed identity. Only the minimum necessary amount of data will be requested from the individual to validate the match.
- 30. The data returned to the government service that initiated the identity verification check on the individual will include the result of the identity check, and a minimum set of attributes required to identify the individual whose identity was checked. For example, this might include the individual's name, date of birth, and any additional data attributes that the government service requested were collected from the individual, such as the individual's address.
- 31. In line with the Code of Practice and prior to sharing any data, all parties to the data share will complete an agreed business case, information sharing agreement, data protection impact assessment and security plan which will specify the data items to be shared. Data sharing will take place in accordance with data protection legislation, UK GDPR, the Commissioners for Revenue and Customs Act 2005, the Information Commissioner's Office Data Sharing Code of Practices and all other relevant statutory guidance and codes of practice.
- 32. All public authorities who are parties to the data sharing will continue to ensure that data is held securely, to the appropriate security and information management standards, maintained to the appropriate quality, used only for the specified purpose of identity verification services, kept as long as required for the specified purpose of identity verification services, and then securely deleted.

6

https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/

- 33. Any and all data shares under the proposed objective will be included in the Register of information sharing agreements⁷ established under the Digital Economy Act 2017.
- 34. As part of the verification process provided by GOV.UK One Login, checks will be made to assure a user's identity and ensure that the identity is not fraudulent or being misused. This protects the individual, ensuring that their identity is not used to access services on their behalf without their permission.
- 35. If the outcome of these checks is that GOV.UK One Login suspects the user is not the identity they claim to be, the service will alert the relevant service or government department. GOV.UK One Login will not take punitive action. It will protect against fraud by making identity theft more difficult by including many more digital checks than under the current system and protecting access at the gateway to government services.

Question 7 - To what extent do you agree that the data items, known as data attributes, as described under this proposed objective are consistent with, and appropriate for, the delivery of the objective?

Please choose one of the following options:

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree
- Don't know

Please provide the reason for your response and specify the data item you are referring to.

What is the likely impact of the new data sharing power?

- 36. The impact of the new data sharing powers would be to deliver citizen-centric public services that are fit for the digital age, with the right outcomes that are centred on user needs.
- 37. Proposed benefits from the data sharing for individuals and households include:

19

https://www.gov.uk/government/publications/register-of-information-sharing-agreements-under-chapte rs-1-2-3-and-4-of-part-5-of-the-digital-economy-act-2017

- creating easy and consistent ways to access and sign-in to government services, reducing fragmentation and costs, and replacing clerical methods using documentary evidence;
- o improving user experience when accessing government services;
- improving inclusion by expanding identity verification services to those citizens currently excluded because they do not have conventional identity documents such as a passport;
- facilitating simple, faster access to the specific services citizens want to use; and
- o reducing identity fraud and misuse.
- 38. The proposed objective is intended to facilitate data sharing for the purposes of identity verification, thereby improving services for individuals and households. It is not intended as a mechanism to take action in a fraud offence, and will not be punitive. However, public authorities have a duty to protect the public purse and must follow best practice guidance on fraud management.
- 39. Case studies are set out below to illustrate how the data sharing will work.

Case Studies for identity verification services

Mikel

Mikel has secured a job at an international airport and has been asked to apply for a basic DBS check (criminal record check) because he requires an airside pass to allow him to work in restricted zones.

Mikel needs to prove his identity before he can request a DBS check. He begins this process by first creating a GOV.UK One Login account using his email address, choosing a secure password, and setting up two-factor authentication.

Mikel then enters the details of his UK driving licence. The details of his driving licence can then be checked against government records to ensure the details provided by Mikel match.

Mikel then continues the process of proving his identity by answering some security questions based on government information held against him, such as information about his income. This allows him to prove that he really is Mikel and

prevent someone else pretending to be him, because only he should be able to answer the questions correctly.

The outcome of these checks are retained by the identity verification service and can be reused so he doesn't have to perform the same checks in the future when accessing other government services.

Having successfully proven his identity in a few minutes, Mikel continues to request his DBS check.

Bukayo

Bukayo is in the process of remortgaging his property. A conveyancer, on behalf of his lender, has created a mortgage deed for Bukayo and issued it to HM Land Registry, who now makes it available for Bukayo to sign online as part of its digital services

To do this, Bukayo needs to prove his identity to ensure that it's really him signing the mortgage deed, and not anyone else.

Bukayo created a GOV.UK One Login account last year when he needed to manage his tax information on GOV.UK. This involved passing an identity check, the outcome of which was retained to save him having to do it again in the future.

Because Bukayo has already proven his identity, all he needs to do is sign into his GOV.UK One Login account and agree to share his information to the <u>Sign your mortgage deed service</u>.

He continues on to sign the mortgage deed without having to do any additional checks in gov.uk

This section is aiming to ascertain if you perceive any specific groups will be affected by inequalities which arise as a result of the implementation of this objective.

Question 8 - To what extent do you consider the proposed sharing of data for the

identity verification objective will lead to any individual and/or household losing any benefit?

Please choose one of the following options:

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree
- Don't know

Please provide the reason for your response.

Question 9 - To what extent do you consider the proposed sharing of data for the identity verification objective will lead to an individual and/or household losing access to a service?

Please choose one of the following options:

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree
- Don't know

Please provide the reason for your response.

Question 10 - Do you think the proposed data sharing for identity verification services will negatively impact on people who share any of the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

- Yes
- No
- Don't know

If yes, please provide the reasons for your response specifying the protected characteristic(s) you think will be impacted.

Why introduce the power now?

- 40. An increasing number of people are accessing government services online, and they expect these services to be simple, quick, safe and secure; expectation levels for public services have never been higher. A new data sharing gateway will provide legal clarity for public sector organisations to participate in identity verification services.
- 41. The <u>Digital Identity Call for Evidence in 2020</u>8 demonstrated the UK public's strong desire for the government to use digital identities to enable citizens to access products and services with ease, while maintaining privacy protections and safeguards to ensure citizens are protected from fraud. Responses to the call for evidence furthermore highlighted how wide scale adoption of secure digital identity solutions has the potential to reduce the opportunity for organised crime, thereby reducing the opportunity for the theft and use of physical identity documents to access services.
- 42. The government has worked closely with its partners in the public and private sectors to publish guidance on how to prove someone's identity (Good Practice Guide 45)⁹ and how to use authenticators to protect an online service (Good Practice Guide 44)¹⁰. This guidance has been welcomed by the digital identity community, and is a key element of establishing a set of standards and rules that would support interoperability across the UK in a secure and consistent way.
- 43. The benefits of the proposed objective for identity verification services are significant and include improved trust between citizens and government; the infrastructure to unlock hundreds of millions of pounds savings across departments through avoided costs and duplicate digital identity systems; and more and better quality insights for Ministers to inform policy.
- 44. Improved data sharing with stringent privacy and security measures in place is central to transforming the delivery and efficiency of public services and people's ability to interact confidently with government in an increasingly digital world.

https://www.gov.uk/government/consultations/digital-identity/outcome/digital-identity-call-for-evidence-response

⁹ https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

 $^{{\}it https://www.gov.uk/government/publications/authentication-credentials-for-online-government-service} \ s$

What other options have been considered?

45. Government has considered other legislative options and there is no legislation in place specifically to enable data sharing across government for identity verification purposes. Identity verification services currently rely on a variety of different data sharing powers and the draft regulations provide for a single piece of legislation to improve access to services by citizens. Government believes that these draft regulations are necessary to deliver benefits to individuals and households.

How does the data sharing align with UK government priorities?

- 46. Government is committed to improving the government's use of data. The Cabinet Office is committed to driving forward use of the Digital Economy Act 2017 data sharing powers across government to improve public service delivery, as well as addressing barriers to data sharing more widely to improve digital inclusion and promote "levelling up".
- 47. The government announced development of a new cross government <u>single</u> <u>sign-on and digital identity assurance pilot</u>¹¹, as part of the One Login for Government programme. Following the spending review, the government shared a <u>further announcement on the One Login for Government</u> <u>programme</u>¹², and the ambition to build a single way for citizens to prove their identity and access central government services online. Indeed, improved data sharing, supported by the proposed legislation, is critical to the long-term success of the One Login for Government programme.
- 48. The proposed data sharing objective:
 - is complementary to the government's plans set out in Mission 3 of the <u>National Data Strategy¹³</u> to transform the government's use of data to drive efficiency and improve public services;
 - supports Mission 5 of the GDS 2021-2024 strategy¹⁴ to join up data across departments, ensuring data remains at the heart of GDS' strategic approach; and
 - supports <u>Mission 2 of the Central Digital and Data Office's (CDDO)</u>
 <u>Digital and Data Strategy 2022</u> to develop the new digital identity system.

https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy#missions https://gds.blog.gov.uk/2021/05/20/government-digital-service-our-strategy-for-2021-2024/

¹¹ https://questions-statements.parliament.uk/written-statements/detail/2021-04-27/hcws942

¹² https://questions-statements.parliament.uk/written-statements/detail/2022-04-28/hcws797

¹³

49. The Department for Digital, Culture, Media and Sport (DCMS) is developing the <u>UK digital identity and attributes trust framework</u>¹⁵, which encompasses a set of rules and processes that digital identity products and services can choose to meet. DCMS is bringing forward <u>legislation to underpin the trust framework</u>¹⁶, to create effective oversight and governance of those services which follow it, and to enable public authorities to disclose data with those services so governed. DCMS' proposals are focused on enabling digital identity use in the wider economy, while this consultation deals with data sharing within the public sector. The Cabinet Office is collaborating with DCMS to ensure our policy and legislative proposals are complimentary.

Why is the UK Government taking this proposal forward?

50. The UK Parliament approves proposals for new objectives involving disclosure and processing of data held by UK departments. The draft regulations must therefore be taken through the UK Parliament by the UK Government. However, the Cabinet Office is consulting separately with the devolved administrations in Scotland, Wales and Northern Ireland.

Does the data sharing power apply across England, Scotland, Wales and Northern Ireland?

51. The data sharing powers will apply across England, Scotland and Wales. However, PSD data sharing powers have not yet commenced in Northern Ireland.

Will data sharing comply with the relevant data protection requirements?

- 52. Yes, the data sharing will comply with the relevant data protection requirements. The purpose of the underpinning Code of Practice is to provide a set of principles and guidance for the use and disclosure of information under Digital Economy Act 2017 powers. The Code also refers to other requirements when sharing information, including data protection legislation. This requires that data must be processed lawfully, fairly, in a transparent manner and only for specified and legitimate purposes.
- 53. The lawful basis for processing (i.e. sharing) personal data in the proposed objective is that it will be necessary for the performance of a task carried out in the public interest or in the exercise of official authority. The legal power

¹⁵

https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-ver sion

¹⁶ https://www.gov.uk/government/consultations/digital-identity-and-attributes-consultation

underpinning this is section 35 of the Digital Economy Act 2017 where the data is being shared for the purposes of improving and targeting a public service and providing a benefit to individuals and households.

Has GDS carried out a data protection impact assessment?

54. The Code of Practice sets out that public authorities involved in the data share must carry out a data protection impact assessment before sharing data. The data protection impact assessment will assess the potential benefits of the information sharing agreement against the risk or potential negative effects, such as an erosion of personal privacy. Nevertheless, GDS has undertaken data protection impact assessments of the authentication and identity verification processing for GOV.UK One Login it develops. GDS has engaged with the Information Commissioner's Office when developing these assessments.

Does the proposed data sharing comply with current best practice?

- 55. Yes, the proposed data sharing complies with current government practice, including the <u>Data Sharing Governance Framework¹⁷</u>, the <u>Government Data Quality Framework</u>¹⁸, and any initiatives for data standardisation work being taken forward by the <u>Data Standards Authority</u>¹⁹. All parties to the data share will intermittently review the arrangements to ensure that compliance is consistent throughout implementation.
- 56. The Cabinet Office has carried out an initial assessment against the <u>Data Ethics Framework</u> which is published with this consultation. The initial assessment identified no immediate ethical concerns and the complete assessment will be published in due course.

Why consult?

57. The Digital Economy Act 2017, supported by the underpinning Code of Practice requires consultation of certain named individuals, such as the devolved administrations, Information Commissioner and the HMRC Commissioners. It also sets out that, before making regulations, the appropriate national authority, in this case the Cabinet Office, must also consult such other persons as it thinks

¹⁷

https://www.gov.uk/government/publications/data-sharing-governance-framework/data-sharing-governance-framework

¹⁸ https://www.gov.uk/government/publications/the-government-data-quality-framework

¹⁹ https://www.gov.uk/government/groups/data-standards-authority

- appropriate. Collaborative and constructive work has taken place across government to date at official level to take this public consultation forward.
- 58. In any event, we are undertaking a public consultation on this proposed amendment to the regulations so we can be confident that all persons who might reasonably be considered appropriate to be consulted, have been consulted. This will ensure as wide a range of views as possible is considered and factored into the regulations before they are presented to Parliament for approval.

Question 11 - Do you have further comments on this proposed objective?

Impact Assessments

- 59. To ensure that all intended and unintended effects of the draft regulations have been considered and mitigations established, the Cabinet Office has carried out the following impact assessments:
 - A Public Sector Equality Duty assessment against the potential for effects on individuals with protected characteristics as defined under the Equality Act 2010. The assessment found no discrimination against any of the protected characteristics either directly or indirectly and also highlighted positive impacts on the basis of disability, age, gender reassignment as well as on individuals from low socio-economic groups and those without access to a passport and/or driving licence. Positive impacts include allowing individuals to draw on a wide range of data sources to successfully prove their identity online to access government services online, to reuse their identities to access different government services and reduce the need for in-person identity proofing procedures.
 - An assessment against the Better Regulation Framework has found that the draft regulations will not result in any direct costs to businesses.

Furthermore, there will be no financial impacts on local authorities or council tax payers as a result of the draft regulations.

Questionnaire

60. We would welcome responses to the following questions.

Reference	Questions to consider	
	: The Identity Verification Services objective in relation to the three f the Digital Economy Act 2017.	
1	The first condition for new objectives under section 35 of the Digital Economy Act 2017 is that the data sharing should either;	
	a) improve or target a public service provided to individuals or households; or b) provide a benefit (whether financial or otherwise) to individuals or	
	households.	
	To what extent do you agree that the proposed new objective meets at least one of those parts of the first condition?	
	Please choose one of the following options: • Strongly agree • Agree • Neither agree nor disagree • Disagree • Strongly Disagree	
	Don't know	
	Please provide the reason for your response.	
2	The second condition is that the data sharing should improve the well-being of individuals or households.	
	To what extent do you agree that the proposed new objective meets this second condition?	
	Please choose one of the following options: • Strongly agree	
	AgreeNeither agree nor disagree	
	DisagreeStrongly Disagree	

	• Don't know	
	Don't know	
	Please provide the reason for your response.	
3	The third condition is that the data sharing should support the delivery, administration, monitoring or enforcement of a service provided by a particular public authority (or authorities).	
	To what extent do you agree that the proposed new objective meets this third condition?	
	Please choose one of the following options: • Strongly agree • Agree • Neither agree nor disagree • Disagree • Strongly Disagree • Don't know	
	Please provide the reason for your response.	
Section two	: Digital Economy Act 2017, schedule 4	
4	To what extent do you agree that the following government departments should become a public body eligible to share data for public service delivery objectives (these public authorities are listed in Schedule 4)?	
	 Cabinet Office Department for Transport Department for Food, Environment and Rural Affairs Disclosure and Barring Service 	
	Please choose one of the following options: Strongly agree Agree Neither agree nor disagree Disagree Strongly Disagree Don't know Please provide the reason for your response and specify which public	
	body you are providing views on.	
5	To what extent do you agree that the following government	

departments should be able to share data for the identity verification objective?

• Cabinet Office

- Department for Transport
- Department for Food, Environment and Rural Affairs
- Disclosure and Barring Service

Please choose one of the following options:

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree
- Don't know

Please provide the reason for your response and specify which public body you are providing views on.

Are there any other public authorities not proposed in this consultation which you think should be able to share data for the identity verification objective?

Please choose one of the following options:

- Yes
- No

Please provide the reason for your response.

Section three: The identity verification services proposal in relation to the provisions of the Digital Economy Act 2017

To what extent do you agree that the data items, known as data attributes, as described under this proposed objective are consistent with, and appropriate for, the delivery of the objective?

Please choose one of the following options:

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree
- Don't know

	Please provide the reason for your response and specify the data item you are referring to.
Section four	Equality implications
8	To what extent do you consider the proposed sharing of data for the identity verification objective will lead to any individual and/or household losing any benefit? Please choose one of the following options: • Strongly agree • Agree • Neither agree nor disagree • Disagree • Strongly Disagree • Don't know
	Please provide the reason for your response.
9	To what extent do you consider the proposed sharing of data for the identity verification objective will lead to an individual and/or household losing access to a service? Please choose one of the following options: • Strongly agree • Agree • Neither agree nor disagree • Disagree • Strongly Disagree • Don't know Please provide the reason for your response.
10	Do you think the proposed sharing of data for the identity verification objective will negatively impact on people who share any of the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)? • Yes • No • Don't know

	If yes, please provide the reasons for your response specifying the protected characteristic(s) you think will be impacted.
Section five	: Further comments
11	Do you have further comments on this proposed objective?
Section six:	Data Protection
12	Please indicate whether you are happy for the relevant points and comments you have made to be published in the consultation summary report:
	 I am happy for my responses to be published alongside my name and organisation I am happy for my responses to be published alongside my organisation I am happy for my responses to be published anonymously I do not want any of my responses to be published

Timetable

61. A provisional timetable for introducing the power is set out below. Please be aware this may be subject to change as we will progress through the parliamentary process. A final timetable will be confirmed following the consultation period and published on GOV.UK.

Provisional timetable for the parliamentary process

Activity	When
Draft laying date for the Statutory Instrument	July 2023
Enactment of powers	October 2023

Data sharing in place	December 2023
-----------------------	---------------

Thank you for participating in this consultation exercise.

Contact details and how to respond

For information about how we treat your personal data when you respond to our consultation, please see the **Privacy Notice at Annex 5**.

If you need a paper copy or alternative format of this consultation, please contact the Data Sharing Legislation Team, Cabinet Office at dea-data-sharing@digital.cabinet-office.gov.uk

Complaints or comments

If you have any complaints or comments about the consultation process you should contact the Data Sharing Legislation Team, Cabinet Office at dea-data-sharing@digital.cabinet-office.gov.uk.

Confidentiality

If you want the information that you provide to be treated as confidential, please explain to us why you regard the information you have provided as confidential. We will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Cabinet Office.

Annex 1 - Draft Digital Government (Disclosure of Information)(Identity Verification Services) Regulations - see separate document

See separate document

Annex 2 - Background to identity verification services

- 1. The Government Digital Service (GDS), in collaboration with other government departments, is developing a digital identity verification service as part of the One Login for Government programme²⁰. The service will be named GOV.UK One Login.
- 2. GOV.UK One Login will allow people to create and reuse digital identities to access public services. The service will make it easier for people to find and access government services, allow users to prove their identity online, protect the privacy of users and reduce identity fraud and theft.
- 3. GOV.UK One Login will, over time, replace GOV.UK Verify and other existing systems across government, unifying how users prove their identity online to access government services.
- 4. In order for GOV.UK One Login to fulfil its long-term ambitions, participating public sector organisations will need to be able to check and share several types of government-held personal data to allow users to prove they are who they say they are.
- 5. The current framework does not provide all departments involved with the necessary degree of legal certainty to participate in this important initiative to improve public services. GDS therefore wishes to create a robust legal gateway that will allow participating public sector organisations to share data for the purposes of enabling identity verification services. The Cabinet Office is seeking to achieve this by establishing a new public service delivery objective under section 35 of the Digital Economy Act 2017.
- 6. Furthermore, GDS needs to access a broader range of government-held data sources to improve digital inclusion and promote levelling up. Without a firm legislative basis for these additional sources, there is a risk that certain demographics will not be able to access online public services.
- 7. To underpin the identity verification service and to facilitate access to online services we need to legislate for several types of data sharing:
 - a. checks against documents typically used in identity verification and which are already instrumental to existing systems.

35

²⁰ https://gds.blog.gov.uk/2022/08/24/an-update-on-one-login-for-government/

- b. checks against other information to supplement the identifying documents above to build confidence in the user's identity and allowing people without passports and driving licences to access services.
- c. sharing the results of checks that other government departments or services have already performed, as well as the supporting data, so that users only need to prove their identity once.
- 8. The proposed legislation will provide individuals with simple access to public services. This will be enabled through the GOV.UK One Login system. This new objective will pave the way for effective data sharing across government and improved delivery of public services.
- 9. GOV.UK One Login will make it easier for individuals to find and access government services, will allow citizens to prove their identity only once to a specified level of confidence and will protect the privacy and security of users.

Annex 3 - Background to the Digital Economy Act 2017

What is the Digital Economy Act 2017?

1. The Digital Economy Act 2017 contains a single, umbrella piece of legislation designed to reduce legal barriers to data sharing and enable public authorities to share personal information for specific purposes. Data sharing provisions are set out in Part 5 to the Digital Economy Act 2017. The Digital Economy Act 2017 is used where there are no other statutory gateways and where common law powers cannot be relied on or is not appropriate.

Why and how did we develop the legislation?

- 2. The Digital Economy Act 2017 was introduced following the The Law Commission scoping report of July 2014 'Data Sharing Between Public Bodies'. The report described the complex legal landscape around data sharing that impedes government's ability to respond quickly and effectively to the complex problems that people need help with. Where powers did not exist, it could take years to establish legislation to introduce new data sharing powers.
- 3. The data sharing chapters of the Digital Economy Act 2017 were developed through an open policy making process working collaboratively with over 50 public sector, civil society and privacy organisations for more than two years.
- 4. The data sharing provisions in the Digital Economy Act 2017 now allow public authorities to access data to deliver better services without the considerable delays required to create new legal powers by primary legislation.

What do the public service delivery powers do?

5. The public service delivery powers allows for data sharing to support services and positive interventions for citizens and households as part of social and economic policies. Examples include supporting individuals and households with multiple disadvantages and/or living in fuel/water poverty. See the regulations which created these objectives.

What does the Public Service Delivery Review Board do?

- 6. The <u>Public Service Delivery Review Board</u>²¹ reviews proposed data sharing objectives to improve and target public services for non-devolved and England-only data sharing. The board then makes recommendations to the relevant Cabinet Office Minister about whether a proposed data sharing objective should be added to the regulations. The relevant Minister for the public service delivery powers is the Minister for the Cabinet Office.
- 7. The Review Board consists of senior officials from relevant information governance or social policy areas from across government and is attended by representatives from the Information Commissioner's Office and invited members from public representative bodies.

Does the Digital Economy Act 2017 align with data protection legislation?

8. Yes, the data sharing provisions of the Digital Economy Act 2017, the regulations made under it, and Codes of Practice all align with UK data protection legislation including the UK GDPR. This is especially important when considering open and transparent use of personal data - see below. The Digital Economy Act 2017 provides the statutory gateway for public authorities who need to share data for a public task, which is one of the lawful bases in the UK GDPR. In using this statutory gateway, public authorities are required to comply with the data protection principles as laid out in the UK GDPR.

Who uses the Digital Economy Act 2017?

9. Public authorities who are specifically included in each chapter and its accompanying Schedule use the Digital Economy Act 2017 to share data for specified purposes. Using the powers is permissive, that is, the public authority has the discretion to decide whether to disclose data or not, with the exception of chapter 7 relating to statistics. Health and adult social care bodies are not currently included in the scope of the Digital Economy Act 2017.

Is the government committed to being open and transparent about data shared under the Digital Economy Act 2017?

²¹ https://www.gov.uk/government/groups/digital-economy-act-public-service-delivery-review-board

10. Yes, the government is committed to being open and transparent by making information about data shared under the Digital Economy Act 2017 easily available to all to find and understand. This helps citizens, the government and the Information Commissioner's Office understand what data sharing is taking place. Public authorities using the public service delivery power must add data shares to the <u>public register</u>²². The Cabinet Office is responsible for maintaining the register and the Public Service Delivery Review Board oversees strategic consistency.

Annex 4 - public authorities who would be able to share data for the purposes of the proposed identity verification services objective

English and UK wide bodies
Home Office
Ministry of Justice
The Lord Chancellor
Ministry of Defence
HM Revenue and Customs
Department for Levelling Up, Housing & Communities
Department for Education
Department for Work and Pensions
Department for Business, Energy and Industrial Strategy
Department for Digital, Culture, Media and Sport.

22

https://www.gov.uk/government/publications/register-of-information-sharing-agreements-under-chapte rs-1-2-3-and-4-of-part-5-of-the-digital-economy-act-2017

HM Land Registry

An organisation which provides services to a specified public authority in connection with the specified objective

A county council in England

A district council in England

A London borough council

A combined authority established under section 103 of the Local Democracy, Economic Development and Construction Act 2009

The Common Council of the City of London in its capacity as a local authority

The Council of the Isles of Scilly

The Greater London Authority

Welsh bodies

The Welsh Ministers

The Welsh Revenue Authority

A county council in Wales

A county borough council in Wales

A community council in Wales

A person providing services in connection with a specified objective (within the meaning of section 35) to a specified person who (a) falls within this part of this Schedule; and (b) is a public authority.

Scottish bodies

The Scottish Ministers

A council constituted under section 2 of the Local Government etc. (Scotland) Act 1994.

A person providing services in connection with a specified objective (within the meaning of section 35) to a specified person who (a) falls within this Part of this Schedule; and (b) is a public authority.

New public authorities to be added to Schedule 4

The Cabinet Office

Department for Transport
Department for Environment, Food and Rural Affairs
Disclosure and Barring Service

Annex 5 - Privacy Notice

This notice sets out how we will use your personal data, and your rights. It is made under Articles 13 and/or 14 of the UK General Data Protection Regulation (UK GDPR).

Your data

Purpose

The purpose(s) for which we are processing your personal data is to conduct a public consultation which is a statutory requirement when introducing objectives under the Digital Economy Act 2017, the public service delivery power.

We are accepting responses online using SmartSurvey and via email.

Respondents may contact us to arrange postal responses on a case-by-case basis.

We strongly encourage respondents to use SmartSurvey to fill in an online survey where reasonably practicable.

Postal and email responses will be subject to the same safeguards as digital responses, ensuring secure handling, storage, retention and destruction.

The data

We will process the following personal data:

- name (optional)
- email address (optional)
- whether you are responding as an individual or on behalf of an organisation (mandatory)
 - if so, the name of your organisation (mandatory)
 - the sector that your organisation best identifies with
- your opinions about the Identity Verification Services objective proposal.

We have provided free text boxes for each question where you will be able to explain your responses. If you have opted to remain anonymous, we ask that you refrain from providing any personal information which may identify yourself or another individual.

Use of personal data

Providing name and email address are not mandatory, respondents can choose to proceed to respond anonymously.

If you do provide this information if appropriate, we will attribute any published comments or feedback to you and your organisation. This means that your personal information will be included in the government response paper.

We may also wish to make further contact with you, should we need to discuss your feedback and comments. This is a crucial part of policy making, and it allows us to fully engage with respondents and external stakeholders.

There is also a possibility with a public consultation that the consultation would produce a net negative response, resulting in the policy returning to the drafting stage. In that event, those participants who voiced concerns or disagreed with particular aspects of the consultation would be invited to take part in conversations/roundtable discussions to address these issues before the consultation would be relaunched.

As part of the consultation exercise, we will ask you for your opinions by means of free text boxes. If you have opted to remain anonymous, we request that you refrain from providing sensitive data which may identify yourself or another individual.

Any personal data that might link an individual to opinions may be published in the government response paper, unless you have opted out.

Publishing

If it is beneficial to the process, we would look to publish your responses attributed to you. This means your personal details that you have provided will be stated in public documentation. If you do not wish this to happen, section 6, question 16 in the survey will request that you declare your preferences, this is where you can request us not to publish your personal information.

If you prefer to respond via email or post, we request that you explicitly state your preferences in relation to publication prior to submission.

Legal basis of processing

The legal basis for processing your personal data is that it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller. In this case that is to conduct a public consultation which is a statutory requirement when introducing a new objective under the Digital Economy Act 2017, the public service delivery power.

Postal responses

Respondents are advised to make arrangements with the Central Digital and Data Office in advance to submit postal responses to the consultation. We request that you correspond with us via email to discuss submission of postal responsesdea-data-sharing@digital.cabinet-office.gov.uk or contact us on 07584 342684. If you choose to submit a postal response, we request that you contact us to make arrangements and post your response before the end of the consultation period.

Hard copy information will be subject to the same arrangements as the electronic responses including limited access, secure retention and destruction policy. We do not intend to retain hard copy materials beyond a 30-day period from the end of the consultation. In a situation where additional details may be provided by mail respondents, for example a return address, we will not retain these data items and they will be subject to secure destruction.

Email responses

Respondents will also be able to submit email responses to dea-data-sharing@digital.cabinet-office.gov.uk

We request that you include the following, 'Response to the consultation on the data sharing for identity verification services' in the subject line if you choose to respond in this way.

Recipients

Your personal data will stay within the Cabinet Office.

As your personal data will be stored on our IT infrastructure, it will be provided to our data processors who provide email, and document management and storage services.

The personal data submitted online on SmartSurvey will be collected by a third party as a contracted data processor. Once collated, the survey data will be extracted to be stored on our corporate IT infrastructure.

As part of the Smart Survey process your personal data may leave the UK. We have put in place appropriate safeguards to minimise any risks to your personal data if it leaves the UK. For more information on how Smart Survey will secure your data, please see the SmartSurvey Privacy Notice on their website.

Retention

We are intending to retain the data until at which time the legislation has successfully passed through Parliament and we perceive no risk of judicial review. However, we do not intend to retain the data beyond 7 years.

Hard copies of the data (postal responses) will be transferred into our IT system and will be destroyed within 30 days of the end of the consultation.

Your rights

You have the right to request information about how your personal data are processed, and to request a copy of that personal data.

You have the right to request that any inaccuracies in your personal data are rectified without delay.

You have the right to request that any incomplete personal data are completed, including by means of a supplementary statement.

You have the right to request that your personal data are erased if there is no longer a justification for them to be processed.

You have the right in certain circumstances (for example, where accuracy is contested) to request that the processing of your personal data is restricted.

You have the right to object to the processing of your personal data where it is processed for direct marketing purposes.

You have the right to object to the processing of your personal data.

International transfers

As your personal data is stored on our IT infrastructure, and shared with our data processors, it may be transferred and stored securely outside the UK. Where that is the case it will be subject to equivalent legal protection through an adequacy decision or reliance on Standard Contractual Clauses.

Contact details

The data controller for your personal data is the Cabinet Office. The contact details for the data controller are: Cabinet Office, 70 Whitehall, London, SW1A 2AS, or 0207 276 1234, or publiccorrespondence@cabinetoffice.gov.uk.

The contact details for the data controller's Data Protection Officer are: dpo@cabinetoffice.gov.uk.

The Data Protection Officer provides independent advice and monitoring of Cabinet Office's use of personal information.

Complaints

If you consider that your personal data has been misused or mishandled, you may make a complaint to the Information Commissioner, who is an independent regulator. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, or 0303 123 1113, or icocasework@ico.org.uk. Any complaint to the Information Commissioner is without prejudice to your right to seek redress through the courts.

[inside of back cover – please leave this page blank]

This document is available in large print, audio and braille on request. Please contact the Data Sharing Legislation Team:

dea-data-sharing@digital.cabinet-office.gov.uk

OGL

© Crown copyright 2018

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit

nationalarchives.gov.uk/doc/open-government -licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

Any enquiries regarding this publication should be sent to us at dea-data-sharing@digital.cabinet-office.gov.uk

This publication is available at www.gov.uk/government/publications

Printed on paper containing 75% recycled fibre content minimum.