Cabinet Office

Government response to the consultation on draft legislation to support identity verification

This response is published on 23 May 2023

Government response to the consultation on draft legislation to support identity verification

Response to consultation carried out by Cabinet Office.

Contents

Executive summary

This Government is committed to transforming the delivery of public services, so that they are easier to use, joined-up, secure and provide better value for money to the taxpayer. Ensuring that these services are available online - to as many people as possible - is central to the Government's approach. We live in a digital age, and people expect their online interactions with government to be seamless.

As has long been the case, accessing services online requires users to prove who they are digitally, just as we need to prove that 'we are who we say we are' when dealing with government in person. This is critical to make sure that the service is provided to the individual who should receive it and to prevent fraud, both against users and the public sector. As part of this, a small number of checks need to be made against trusted data sources, such as validating the person's passport details.

From January to March 2023 we consulted on draft regulations to create a new objective under the existing Digital Economy Act 2017 to enable more effective online identity verification when accessing government services. This is fully consistent with the powers under this Act, which was passed by Parliament in 2017 to give government the flexibility to introduce new data sharing gateways that aid the delivery of key services, as the need arises, via secondary legislation after carrying out consultation.

The public consultation also set out how the proposed objective would support unlocking the full benefits of the new cross-government system known as GOV.UK One Login. This is replacing many legacy government systems so that users will be able to log in to a single account, prove they are who they say they are once and then access all of the government services they require.

GOV.UK One Login is already operational and successfully providing users with access to an initial set of government services, but the new regulations will enable checks against a broader range of trusted data that is already held by participating public bodies. This means that more people, currently excluded from online routes, will be able to access services digitally. The proposed change will also underpin the ability of users to reuse their identity on GOV.UK, once proven, so that they can access a whole range of other government services more simply and efficiently. Government will continue to provide offline channels for users to prove their identity.

We received 66,233 responses to the consultation. We have read them all and this document addresses the points raised by respondents.

We thank the Information Commissioner’s Office and the devolved administrations for their support of the draft regulations and note that some other respondents recognised the benefits to individuals of improved and more inclusive services.

Most of the interest in the consultation expressed strong concerns around identity cards, including incorrect interpretations that a change to the Digital Economy Act 2017 could result in compulsory digital identity. The Government understands that there isn't public

support for identity cards in the UK. The Government remains committed to realising the benefits of individuals being able to identify themselves online in order to access public services. There are no plans to introduce mandatory digital identity.

The majority of responses raised concerns around data privacy. We understand that people rightly want to protect their personal information, and can confirm that this is central to the government's approach. The proposed regulations only relate to using data for the purposes of identity verification and any public body seeking to use the regulations would do so within the clear and robust framework for data sharing set out within the Digital Economy Act 2017 and the UK's robust data protection legislation. The public bodies listed in the consultation are those bodies that either hold information used to verify someone is who they say they are, or that will enable people to access their services.

Where responses did engage with the specific consultation questions, there was a rich set of opinions to analyse which have led to the following changes and provision of additional information.

- Updating the wording of the proposed objective to state that the physical, mental, emotional, social or economic well-being of individuals will be improved. This ensures alignment with the existing 'multiple disadvantages' objective.
- Updating the date that the regulations will come into force to 21 days, rather than the day after being approved by Parliament.
- Updating the Public Sector Equality Duty. The Government remains committed to providing an inclusive and accessible digital identity system, and making services more accessible to more people is a key driver of this change in legislation. We have reviewed the public sector equality duty assessment in the light of feedback, to encompass Gypsy, Roma and Traveller communities.
- Committed to publishing further information on how GOV. UK One Login, will operate within the regulations and overall data protection framework.

The revised Public Sector Equality Duty assessment is published with this government response.

We would like to thank those who replied to the consultation. We will continue to work in close collaboration with representative stakeholder groups to enable more people to use more services online and improve inclusion.

Introduction and contact details

This document is the post-consultation report for the consultation paper on draft legislation to support identity verification.

It will cover:

- the background to the report
- a summary of the responses to the report
- a detailed response to the specific questions raised in the report
- the next steps following this consultation.

Further copies of this report, the consultation paper and alternative formats can be obtained by contacting The Data Sharing Legislation team 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 Cabinet Office at dea-data-sharing@digital.cabinet-office.gov.uk

Background

The consultation paper on draft legislation to support digital identity verification was published on 4 January 2023. It invited comments on the Cabinet Office's draft regulations to enable data sharing between specified public authorities to support delivery of identity verification services to individuals or households.

The consultation paper set out proposals to create a new objective in regulations under Chapter 1 of Part 5 of the Digital Economy Act 2017. The proposed objective will enable data sharing by specified public authorities currently included in Schedule 4 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.

The proposed legislation will allow specified public bodies to process an individual's relevant data (such as driving licence information) when it is necessary for that individual to prove their identity in order to access a government service.

The consultation was live on the GOV.UK website for all UK citizens to review and respond to. In accordance with consultation principles and to ensure transparency and consistency of approach, all consultations are housed on the Government's single web platform - GOV.UK. The consultation was highlighted by a news story on the GOV.UK website and a further blogpost, Helping more people to prove their identity online, was published on 24 February 2023. People were able to respond by an online survey, email or post.

The public consultation is one part of the wider engagement process for considering the new regulations which are drafted to help deliver digital government services to those who choose to use them. This has also included working closely with groups that represent and advocate on behalf of citizens who do not have access to the internet, to capture the views of those less able to engage with government digitally. We held 4 roundtable discussions in February 2023 which were attended by 25 attendees from 20 representative organisations, including the Information Commissioner's Office and some civil society groups.

The consultation period closed at 11:45pm on 1 March 2023 and this report summarises the responses, including how they influenced the final shape of the draft regulations.

Respondents also commented on the impact assessment for people with protected characteristics. We have updated the assessment in line with the comments received and publish it alongside this government response.

A list of responding organisations is at Annex A.

Summary of responses

The consultation on identity verification services received 66,233 responses. Of these responses, 99% came from individuals and 1% from organisations representing the views of many other people. The vast majority of responses (45,249, 68%) came through the online survey, but 20,963 (32%) were received via the email address provided in the consultation. A further 21 responses were received by post. A small number of emailed responses provided a question-by-question response, but almost all (20,929) gave an overall opinion on our proposals.

Identity cards

Many of the individuals who responded to the consultation said they were against digital identity in principle and against identity cards in particular. The consultation on draft regulations to help more people prove their identity online did not include proposals that would introduce identity cards or make digital identities compulsory. Government understands that there isn't public support for identity cards in the UK and remains committed to realising the benefits of digital identity without creating identity cards. The government's position on physical identity cards remains unchanged. There are no plans to introduce mandatory digital identity.

Statutory consultees

The Digital Economy Act 2017, supported by the underpinning Code of Practice, requires consultation with certain authorities such as the devolved administrations, Information Commissioner and the Commissioners for His Majesty's Revenue and Customs (HMRC).

The Information Commissioner's Office

The Information Commissioner's Office did not respond formally to the public consultation. This was because the Information Commissioner's Office regards the legislation to be limited in scope and clear in its explanation for how it will be used.

Devolved administrations

The Scottish Government notes that the design of the objective is very specific to identity verification and supports adding Scottish Ministers and Scottish Local Authorities to the new objective. The Scottish Government supports this approach, on the basis that this is used to help to ensure that users in Scotland have a better experience in the way that they access digital identity services run by Scottish and UK Governments. The Scottish

Government considers the aim of doing this would be to deliver an efficient and accessible service that potentially avoids the need for a user to repeatedly verify their identity; and gives users greater control over their own information and attributes, in order to access the online services and benefits they are entitled to.

The Welsh Government also supports the proposed regulations, highlighting that rollout of effective digital identity verification services, based on verified data held by public authorities, should help improve access to public services by individuals. The Welsh Government also considers that the rollout will also reduce the need for individuals to prove their identity multiple times to different organisations, and provide more seamless access to public services. However, the Welsh Government also identified that public authorities should take steps to ensure citizens fully understand what their data is being used for, and the benefits derived if they do choose to engage with identity verification services.

Although the data sharing powers of the Digital Economy Act 2017 do not currently extend to Northern Ireland, the UK Government has consulted on the draft regulations and remains in close liaison on how they may apply there in the future.

HMRC Commissioners

HMRC Commissioners are content with the draft regulations.

Government response to comments from statutory consultees

Government welcomes confirmation from the Information Commissioner's Office and devolved administrations that the draft regulations are clear and specific to online identity verification services. Government also notes that the HMRC Commissioners are content with draft regulations.

Responses from civil society organisations

We received responses from 5 civil society organisations as set out in Annex A. Comments focused on querying the benefits to individuals and the perceived lack of data safeguarding details included in the regulations, as well as the operation of the government identity verification system, known as GOV.UK One Login.

Government response to comments from civil society organisations

Government notes that the benefits to individuals can be wider than those specified in clause 3b of the draft regulations and will therefore amend the clause to add physical and social well-being as part of the objective. The amended wording specifies improving physical, mental, emotional, social or economic well-being reflects the wording in the existing "multiple disadvantages" specified objective in the public service delivery powers

of the Digital Economy Act 2017 which targets assistance to individuals or households who are affected by multiple disadvantages. Specified objectives under the public service delivery power must benefit either individuals or households. As the draft regulations primarily benefit individuals, they do not include references to households.

Data protection and data sharing under the Digital Economy Act 2017.

On the level of detail of how personal data will be safeguarded in the draft regulations, data sharing powers under the Digital Economy Act 2017 operate within very tight constraints of the overarching data protection legislation, UK GDPR, the Human Rights Act 1998, the Information Commissioner's Office Data Sharing Code of Practice, the 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 Digital Economy Act 2017. The Information Commissioner's Office reported on the strength of the overarching framework in the audit review published in March 2023, concluding as follows:

> The Information Commissioner's Office
>
> Data sharing under the Digital Economy Act provides a supportive framework that includes robust safeguards to share data responsibly for initiatives benefiting the public.

Data sharing under the public service delivery powers of the Digital Economy Act 2017 is permissive, that is, the public body has the discretion to decide whether to disclose data or not. Only the public bodies specified in the regulations would be able to process data for the specified purpose of identity verification services. The public bodies listed in the consultation are those bodies that either hold information used to verify someone is who they say they are, or that will enable people to access their services. Some public bodies will do both, i.e. they hold information, but also will need to verify an individual is who they say they are before they can access a service. Any data sharing arrangement established between the specified public bodies will be required to factor the necessary data flows and ensure they meet data protection principles of proportionality and data minimisation.

Being supported by better cross-departmental data sharing will mean government identity verification services will be as inclusive and accessible as possible for people who struggle to use traditional proofs of identity such as passports and driving licences. However, use of this new objective does not change or undermine the existing data protection laws, requirements or regulations. All data sharing under the regulations must comply with existing data protection legislation. All parties to the data sharing must ensure that personal 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 only as long as is required for the specified purpose of identity verification services and then securely deleted. Government therefore does not believe there is a need to include more detail in the secondary regulations themselves.

However, the Government recognises that specified public bodies as well as citizens themselves would value more published information on how any system which helps people prove who they are online will operate within the data protection legislation. Any government identity verification service that uses these regulations will therefore publish clear information on the use of and access to personal data, starting with GOV.UK One Login. In particular, information will set out which departmental services are using identity verification services to support delivery and which departments will provide data to help the Cabinet Office establish a verified identity. The Government will also amend the draft regulations so that they will come into force 21 days rather than the day after being approved by Parliament.

We also received a joint response from the Local Government Association, SOLACE and SOCITM on behalf of local councils. Local councils agreed that data sharing for identity verification will provide a benefit for individuals if it is implemented inclusively and with local government integrated from the earliest possible point - as both a data holder and a service provider and with the minimum burden on local councils. Government also welcomes comments made by local councils relating to integration with GOV.UK One Login, which will be addressed in further information on how GOV. UK One Login, will operate within the regulations and overall data protection framework.

Responses from individuals and other organisations: scale and methodology for analysis

The consultation was on draft regulations for a data sharing objective to support the way the Government would deliver online identity verification services, which is a Government priority as set out in Mission 2 of Transforming for a digital future 2022-2025: roadmap for digital and data. The questions provided respondents with the opportunity to express their views on the conditions that attach to the regulations and the potential societal impacts. They provided an opportunity to express agreement or disagreement and to raise any perceived impacts, benefits or disadvantages to individuals.

However, there is clear evidence that, of those who responded to the consultation, either by the online survey or by email, many appear to have been significantly influenced by commentaries against implementing compulsory citizen digital identity in principle and data sharing to support it. For example, we noted that 75% of the emails received used one of a small number of templates and a small proportion of these emails (4%) in template format were against identity verification services in principle, and were responding to a much broader issue around digital identity and data sharing than was in scope of this consultation.

The majority of individuals who responded to the consultation commented on wider issues rather than addressing the specific questions on the data sharing regulations that were asked. For example, responses included comments that identity verification services would mean citizens would not be able to use cash, that they would support a social credit

system, that they would lead to an identity card being introduced, or that digital identities are going to be made mandatory for all people. As these wider matters were not part of the consultation, we determined these responses on wider issues to be out of scope for analysis.

Our analysis methodology was to count a question response as against identity verification services in principle if their comments indicated that they were against any form of compulsory citizen digital identity or the data sharing to support it, or if their opposition was based on claims which were not substantiated by the facts set out in the consultation. For the purposes of statistical analysis of the specific questions in the consultation, we have not included these responses as they would distort the analysis of responses from those who did. Furthermore we rejected a small number of responses which were offensive and were profane.

Overall, up to 20% of question responses were out of scope, depending on the question. We removed responses individually per question and not entire consultation responses from individuals or organisations. Nevertheless, outside the context of producing the statistical analysis, we have taken these responses into account as part of this consultation exercise. In practice this approach limited the responses that were fully out of scope, and erred on the side of caution in including as many valid responses as possible. This has meant that many commentary related responses have been included in the analysis with a consequential uplift to negative disagreeing responses. Many of the commentary related responses engaged in more detail on at least one question and we included them in our detailed analysis of questions. Percentages may not total 100% due to rounding.

Government will continue to work to address the types of concerns respondents raised in future policy decisions and communications, for example, as we provide more information on how the government solution, GOV.UK One Login, will operate within the regulations.

Responses to specific questions

Where responses did engage with the specific consultation questions, there was a rich set of opinions to analyse. Many of the responses were driven by anti-digital commentaries without engaging with the specific questions. The common reasons were around an underlying mistrust of government use of personal data, data accuracy leading to poor decision making and security of systems against cyber attacks. The vast majority of respondents considered that an individual's data privacy was more important than the benefits of improved public services. These are common themes across responses to all questions and we have not repeated them each time throughout this government response. As a result, some of the analysis statistics appear to be overwhelmingly skewed towards the majority who used the consultation as a vehicle to express these opinions.

While there appears to be a broader sentiment about government use of personal data that goes beyond the proposed regulations, Government is nevertheless committed to ensuring that maximising public service delivery is balanced by compliance with data protection, strong safeguards to protect personal data privacy and robust cyber security.

Digital transformation and the use of online methods to help people prove who they are will make accessing public services far quicker and simpler. The Government has established the Central Digital and Data Office to drive this transformation forward across government departments.

Section 1: the identity verification services objective in relation to the public service delivery power of the Digital Economy Act 2017.

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?

Summary of responses to question 1

We determined that 16% of responses to this question were out of scope.

Of the responses that were in scope, a majority of 73% disagreed or strongly disagreed that the proposed objective would improve or target a service to individuals, or would provide them with a benefit. The main reasons for this were concerns around erosion of data privacy and protection, data security against cyber attacks and a general mistrust in government use of personal data for wider policy issues. For the majority of respondents, these concerns outweighed any improvements in public service delivery.

2% agreed or strongly agreed, respondents recognised that effective services to help people prove who they are online, based on verified data already held by public authorities, would help improve seamless access to public services by individuals. Respondents further highlighted that effective services to help people prove who they are online would benefit individuals by enabling faster access to services. A further service improvement noted was that services would be able to carry out identity checks - and thus provide the benefits of service outcomes to individuals - more quickly.

The remaining 24% neither agreed nor disagreed, or did not know.

Government response to question 1

Government recognises concerns by the majority of respondents on data privacy and security, and wishes to reassure that any data sharing taking place under these new regulations will be secure and safeguard user's data privacy as set out above in data protection legislation and the Digital Economy Act 2017 in particular. Data sharing under

the proposed regulations would adhere to the principle of using the minimum amount of data to help people prove who they are, thus ensuring that less data is processed overall. This activity further minimises the risks posed by data sharing.

To further provide confidence as to the safety and privacy of data sharing under the proposed legislation, any service which helps people prove who they are online will publish information on the use of personal data, starting with GOV.UK One Login.

Government welcomes recognition by a small proportion of respondents that services which help people prove who they are would deliver better, joined-up services with benefits to individuals.

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?

Summary of responses to question 2

We determined that 12% of responses to this question were out of scope.

Of the responses that were in scope, a majority of 76% responses disagreed or strongly disagreed that the proposed objective would improve the well-being of individuals or households. The main reasons for this were concerns around erosion of data privacy and protection, data security against cyber attacks and a general mistrust in government use of personal data for wider policy issues. For the majority of respondents, these concerns outweighed any improvements in public service delivery.

Of those 2% who agreed or strongly agreed, respondents recognised that effective services to help people prove who they are online based on verified data already held by public authorities would reduce the need for individuals to prove who they are multiple times to different departments or services, thus saving them time and reducing frustration in having to provide the same information to different departments and services.

The remaining 22% neither agreed nor disagreed, or did not know.

Government response to question 2

As above, Government notes concerns by the majority of respondents on data privacy and security and wishes to reassure respondents that any data sharing taking place under these new regulations will be secure. Government also welcomes recognition that services to help people prove who they are would help improve individuals health and well-being.

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).

Summary of responses to question 3

We determined that 13% of responses to this question were out of scope.

Of the responses that were in scope, a majority of 75% disagreed or strongly disagreed that the proposed objective would support the delivery of administration, monitoring or enforcement of a service provided by a particular public authority (or authorities). The main reasons were concerns that data protection would be put at risk by data sharing and worries that data sharing would be used to facilitate government monitoring and enforcement of individuals rather than the delivery of public services.

Of those 3% who agreed or strongly agreed, respondents recognised that services to help people prove who they are online would improve service responsiveness and save people's time because of direct access to verified data already held by public authorities.

The remaining 22% neither agreed nor disagreed, or did not know.

Government response to question 3

Government notes concerns on data protection, as above, and confirms that monitoring and enforcement of how well public services are delivered by public bodies does not include monitoring of any citizen's individual activity. Government also welcomes recognition that services to help people prove who they are online would support improved public service delivery and improve their well-being.

Responses to specific questions - section 2: the identity verification services objective in relation to the public bodies who would be able to share personal data.

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 bodies are listed in Schedule 4)?

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

Summary of responses to question 4

We determined that 14% of responses to this question were out of scope.

Of the responses that were in scope, a majority of 89% disagreed or strongly disagreed that the Cabinet Office, Department for Transport, Department for Environment, Food and Rural Affairs or the Disclosure and Barring Service should be able to share data to improve or target public services under specified objectives. The main reasons for this were concerns around erosion of data privacy and protection, data security against cyber attacks and a general mistrust in government use of personal data for wider policy issues.

Of those 6% who agreed or strongly agreed, respondents recognised that the departments listed deliver services to the public and should be able to share personal data to improve those services, subject to privacy safeguards.

The remaining 4% neither agreed nor disagreed, or did not know.

Government response to question 4

Government notes concerns from the majority of respondents on data privacy and welcomes recognition from a small proportion of respondents that the Cabinet Office, Department for Transport, Department for Environment, Food and Rural Affairs or the Disclosure and Barring Service identity verification services should be able to share personal data to improve their services, subject to safeguards.

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 Environment, Food and Rural Affairs**
- **Disclosure and Barring Service**

Summary of responses to question 5

We determined that 14% of responses to this question were out of scope.

Of the responses that were in scope, the majority (93%) of responses disagreed or strongly disagreed that the Cabinet Office, Department for Transport, Department for Environment, Food and Rural Affairs or the Disclosure and Barring Service should be able to share data for identity verification services. The main reasons for this were concerns around erosion of data privacy and protection, data security against cyber attacks and a general mistrust in government use of personal data for wider policy issues. Some considered that public bodies already hold sufficient personal data about the public. Some respondents would welcome further information on which departments would use identity verification services and which would hold data key to verifying a person's identity. In particular, some respondents did not acknowledge that the Department for Environment, Food and Rural Affairs delivered public services. Views on the need for the Disclosure and Barring Service were mixed.

Of those 4% who agreed or strongly agreed felt that identity verification services should be available to the Cabinet Office, Department for Transport, Department for Environment, Food and Rural Affairs or the Disclosure and Barring Service to improve and target identity their services. Respondents acknowledged that the Cabinet Office would need to access cross-government datasets to deliver identity verification services and that the Department for Transport, as the sponsoring department for the Driver and Vehicle Licensing Agency, holds key driving licence data that would support an identity verification service. Some also acknowledged that the role of the Disclosure and Barring Service in helping to make recruitment safer in public services was key to identity verification services.

The remaining 4% neither agreed nor disagreed, or did not know.

Government response to question 5

Government recognises the strong desire for more information on how public bodies would use identity verification services and will therefore publish clear information on use of, and access to personal data for the service, starting with GOV.UK One Login. In particular, information will set out which departmental services are using identity verification services to support delivery and which will provide data to help departments establish who a person is. The Government also welcomes recognition that the Cabinet Office, Department for Transport, Department for Environment, Food and Rural Affairs or the Disclosure and Barring Service should be able to use the data they already hold to improve and target identity verification services, subject to safeguards.

Department for Environment, Food and Rural Affairs (DEFRA) DEFRA offers a number of public services targeted at improving and protecting the environment, growing a green economy, sustaining thriving rural communities and supporting food, farming and fishing industries. Some of these require identity verification services. Government anticipates that approximately 400,000 people will use GOV.UK One Login to access DEFRA services.

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?

Summary of responses to question 6

Some respondents, including the Local Government Association, SOLACE and SOCITM suggested that health and adult social care bodies should be able to share data for identity verification services, although these bodies are not currently in the scope of the Digital Economy Act 2017 for data sharing purposes. There were no other suggestions for further

public bodies not currently listed in Schedule 4 to the Digital Economy Act 2017 to be added for identity verification services.

Government response to question 6

Health and adult social care bodies are not currently included in the scope of Digital Economy Act 2017. On the basis of responses, therefore, we consider that the correct public bodies are included in the scope of the draft regulations.

Responses to specific questions - section 3: the identity verification services objective in relation to the data items to be processed

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?

Summary of responses to question 7

We determined that 11% of responses to this question were out of scope.

Of the responses that were in scope, the majority (87%) of responses disagreed or strongly disagreed that the data items described were consistent with identity verification services. The main reason was concerns about the transparency of the data items listed in the public consultation, particularly special category data and transactional data like income.

Of those 3% who agreed or strongly agreed, respondents recognised that the data items were relevant to delivering effective identity verification services.

The remaining 10% neither agreed nor disagreed, or did not know.

Government response to question 7

Government welcomes recognition that the data items listed in the consultation are consistent with identity verification services, for example, names and addresses that are held by some public bodies when delivering services. However, the Government also notes concerns around transparency in using specific data items and will address these concerns in published information to support operation of the regulations within the underpinning data sharing protection legislation.

Responses to specific questions - section 4: views on equality issues

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?

Summary of responses to question 8

We determined that 12% of responses to this question were out of scope.

Of the responses that were in scope, a minority (25%) responded with disagree/strongly disagree, indicating that they expect no individual to incur loss of benefit of easier access to services as a result of identity verification services. The main reasons cited were that improved access to government services can only benefit individuals and households provided the appropriate privacy controls are in place; that wider public sector data sharing will improve digital inclusion to those currently excluded from easy access to benefits by not having conventional identity documents like passports or driving licences; that using trusted data from authoritative sources would prevent identities being hijacked; and would prevent fraud from entering government services at the earliest opportunity.

Some 58% agreed or strongly agreed, indicating views that they perceive there will be a loss of benefit if identity verification services are implemented. The main reasons cited were concern that use of digital identities could lead to discrimination against marginalised communities, and that those who choose not to use, or who are not able to use, an online verification system may lose out on benefits if online services were to replace other forms of identity verification. Respondents highlighted that some of the most vulnerable members of society have the lowest levels of computer access.

The remaining 17% neither agreed nor disagreed, or did not know.

Government response to question 8

The Government welcomes recognition from some that improved access to government services can benefit individuals, provided the appropriate privacy controls are in place and that sharing data will help prevent hijacked identities by using trusted data from authoritative sources when proving identity. However, Government also notes concerns that some marginalised groups may be unable or reluctant to use online public services. Government will continue to offer offline channels for those users less able to engage with government services to prove their identity.

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?

Summary of responses to question 9

We determined that 17% of questions to this question were out of scope.

Of the responses that were in scope, a minority (29%) responded positively with disagree/strongly disagree, indicating that they expect no individual or household to lose access to a service as a result of identity verification services. The main reasons cited were that improved access to government services can only benefit individuals and households provided the appropriate privacy controls are in place; that wider public sector data sharing will improve digital inclusion to those currently excluded from easy access to services by not having conventional verification documents like passports or driving licences; would prevent fraud from entering government provided services at the earliest opportunity; and would support ease of access to a wider range of public services, ensuring that individuals can more easily interact with government to access the services they may be entitled to.

Some 54% agreed or strongly agreed, indicating views that they perceive there will be a loss of access to services if identity verification services are implemented. The main reasons cited were concern that use of digital identities for accessing government services could lead to discrimination against marginalised communities; those who choose not, or who are not be able to use an online verification system may be delayed in accessing services if online channels were to replace other forms of identity verification. Respondents highlighted that some of the most vulnerable members of society have the lowest levels of computer access. Furthermore, Government will continue to offer offline channels for those users less able to engage with government services to prove their identity.

The remaining 17% neither agreed nor disagreed, or did not know.

Government response to question 9

The Government welcomes recognition that improved access to government services can benefit individuals, provided the appropriate privacy controls are in place and that no individual should lose access to a service as a result of identity verification service. Government also notes the potential for discrimination against marginalised groups in society and has reviewed the Public Sector Equality Duty assessment.

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)?

Summary of responses to question 10

We determined that 12% of responses to this question were out of scope.

Of the responses that were in scope, a majority (83%) indicated that data sharing to support identity verification services would negatively impact on people who share any of the protected characteristics under the Equality Act 2010. Examples cited were marginalised, vulnerable and minority groups who are more likely to have reduced access to online services, for example, people with disabilities, on a low income or those with low digital literacy levels or limited internet access). Some respondents particularly highlighted that migrants and people in Gypsy, Roma and Traveller communities may be particularly impacted.

8% of respondents did not perceive the implementation of the proposed identity verification services would lead to any negative impacts on people who share any of the protected characteristics under the Equality Act 2010. Respondents highlighted that inclusive identity verification services would assist those who may have difficulty in proving their identity and therefore prevent discrimination at the earliest opportunity.

The remaining 9% neither agreed nor disagreed, or did not know.

Government response to question 10

Government carried out an assessment under the Public Sector Equality Duty (PSED) and found no negative impacts on those with protected characteristics under the Equality Act 2010. In the National Data Strategy published in 2020, the Government also recognises that wider use of data has great potential in tackling digital exclusion and creating a fair society for all. For identity verification services, this would include being able to access wider government datasets - beyond passport and driving licence data - to help a user prove their identity, rather than relying on paper documents.

The Government remains committed to providing an inclusive and accessible system that helps people prove they are who they say they are. Government has reviewed the PSED assessment to include consideration of Gypsy, Roma and Traveller communities, which we have published with this government response. Furthermore, Government will continue to offer offline channels for those users less able to engage with government services to prove their identity.

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

Summary of responses to question 11

Respondents made a number of further comments on identity verification services, the broad themes of which are set out below.

Consent to data sharing

Respondents commented that public bodies should not share the personal data they hold for any purposes without prior consent data from the individual.

In relation to identity verification services proposed by the government, the proposed regulations will enable specified public bodies to process an individual's data (such as driving licence information) when it is necessary for them to prove who they are in order to access a government service. Only the minimum number of data checks will be used to verify who a person is. Proving who you are online will not be compulsory; instead people will have more choice as to how they prove things about themselves.

The lawful basis for processing (i.e. sharing) personal data will be determined by the responsible data controllers, but for public services this would typically be that it will be necessary for the performance of a task carried out in the public interest or in the exercise of official authority (Article 6(1)(e) UK GDPR). Section 35 of the Digital Economy Act 2017 provides a legal underpinning for relying on that basis where the data is being shared to achieve a specified objective for the purposes of improving and targeting a public service and providing a benefit to individuals and households.

Bulk data sharing

Respondents commented that the regulations appeared to give rise to data sharing in bulk. However, the proposed regulations will not enable bulk data sharing; rather, they seek to allow data sharing between specified public authorities, limited by the minimum number of data checks to verify who a person is and only for the purposes of identity verification.

Digital currency

The consultation on draft regulations to help more people prove who they are online did not include proposals that would impact on the ability for individuals or households to use cash or to support a digital currency. However, there is another public consultation open until 7 June 2023 launched by the Bank of England and HM Treasury called the digital pound: A new form of money for households and businesses? that is looking for views on introducing a digital pound. Details of how to respond to that consultation are included on GOV. UK.

Conclusion and next steps

The UK Government will take forward the regulations outlined above and in the consultation document as soon as parliamentary time allows.

Annex A – List of respondent organisations

Civil Society organisations who responded to the consultation were:

- Amberhawk Training Ltd
- Big Brother Watch
- Medconfidential
- NO2ID
- Privacy International

Other organisations who responded to the consultation included:

- Area51 Ltd
- Cambridge Montessori Ltd
- Christian Voice
- DECaDE - Centre for the Decentralised Economy
- Feedback CIC
- Good Things Foundation
- Heritage Party
- Kingdom Justice Movement
- Letting Focus
- Local Government Association
- Low Carbon Alliance
- Mastercard
- Mydex Community Interest Company
- Northern Heart
- Open Identity Exchange
- Options for Change Charity
- Payments Association
- Powys County Council
- Rolls Royce PLC
- Society for Innovation, Technology and Modernisation (SOCITM)
- Society of Local Authority Chief Executives (SOLACE)
- Veriff
- Veritas Law
- Workers Party of Britain
- World Innovation Foundation
- XSC Group
- YDK Technologies Ltd

This document is available in large print, audio and braille on request. Please contact dea-data-sharing@digital.cabinet-office.gov.uk

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.