



Department for
Digital, Culture,
Media & Sport

We thank you for your time spent taking this survey.
Your response has been recorded.

Below is a summary of your
responses

[Download PDF](#)

Digital identity and attributes consultation survey

This is the survey for the [digital identity and attributes consultation](#). Please read the proposals before responding to this survey. A summary of questions asked in this survey can be found at the bottom of the document.

The online survey allows you to save a draft response and return to the survey later. You do not have to answer every consultation question and there is a confirmation page before a response is submitted.

Using the online survey greatly assists in our analysis of the responses, enabling more efficient and effective consideration of the issues raised for each question.

The consultation and online survey will last for eight weeks, opening 19 July and closing at 11:59 PM 13 September.

For enquiries about responding to the survey, please contact digital-identity-consultation@dcms.gov.uk. The privacy notice associated with this email can be found [here](#).

Privacy notice:

Who is collecting my data?

The Department for Digital, Culture, Media & Sport (DCMS) helps to drive growth, enrich lives and promote Britain abroad.

We protect and promote our cultural and artistic heritage and help businesses and communities to grow by investing in innovation and highlighting Britain as a fantastic place to visit. We help to give the UK a unique advantage on the global stage, striving for economic success.

Purpose of this Privacy Notice

This notice is provided within the context of the changes required by the Article 13 & 14 of UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA). This notice sets out how we will use your personal data as part of our legal obligations with regard to Data Protection. DCMS' [personal information charter](#) (opens in a new tab) explains how we deal with your information. It also explains how you can ask to view, change or remove your information from our records.

What is personal data?

Personal data is any information relating to an identified or identifiable natural living person, otherwise known as a 'data subject'. A data subject is someone who can be recognised, directly or indirectly, by information such as a name, an identification number, location data, an online identifier, or data relating to their physical, physiological, genetic, mental, economic, cultural, or social identity. These types of identifying information are known as 'personal data'. Data protection law applies to the processing of personal data, including its collection, use and storage.

What personal data do we collect?

Most of the personal information we collect and process is provided to us directly by you. This includes:

- Your name or the name of your organisation, your email address (if you decide to provide these details to us)
- Information on how you use this website. This includes IP address and analytical cookies

How will we use your data?

The personal data we process are the details of individuals who respond to the consultation – name, email address and phone number. This is processed by DCMS for the purposes of the consultation, so we can respond to your queries and views. It may also include using your personal data to invite you to events relating to the consultation. Finally, there may be a need to follow up in the aftermath of the consultation on the same topic or closely related topics.

What is the legal basis for processing my data?

The Data Protection Legislation states that, as government departments, the departments may process personal data as necessary for the effective performance of a task carried out in the public interest (i.e. a consultation). U.K. GDPR Art. 6 (1) e.

What will happen if I do not provide this data?

We will not be able to follow up with you regarding your survey response.

Who will your data be shared with?

Copies of responses may be published after the survey closes. If we do so, unless you indicate otherwise, we will ensure that neither you nor the organisation you represent are identifiable, and any responses used to illustrate findings will be anonymised.

If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this, it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information, 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 Departments.

How long will my data be held for?

Your personal data will be held for two years after the survey is closed. This is so that the department is able to contact you regarding the result of the

survey following analysis of the responses.

Will my data be used for automated decision making or profiling?

We will not normally use your data for any automated decision making. If we need to do so, we will let you know.

Will my data be transferred outside the UK and if it is how will it be protected?

We will not send your data overseas.

What are your data protection rights?

You have rights over your personal data under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

The Information Commissioner's Office (ICO) is the supervisory authority for data protection legislation, and maintains a full [explanation of these rights on their website](#)

DCMS will ensure that we uphold your rights when processing your personal data.

How do I complain?

You can find out more here: [Personal information charter](#)

The contact details for the data controller's Data Protection Officer (DPO) are:

Data Protection Officer

The Department for Digital, Culture, Media & Sport

100 Parliament Street

London

SW1A 2BQ

Email: dpo@dcms.gov.uk

If you're unhappy with the way we have handled your personal data and want to make a complaint, please write to the department's Data Protection Officer or the Data Protection Manager at the relevant agency. You can contact the department's Data Protection Officer using the details above.

How to contact the Information Commissioner's Office

If you believe that your personal data has been misused or mishandled, you may make a complaint to the Information Commissioner, who is an independent regulator. You may also contact them to seek independent advice about data protection, privacy and data sharing.

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Website: www.ico.org.uk

Telephone: 0303 123 1113

Email: casework@ico.org.uk

Any complaint to the Information Commissioner is without prejudice to your right to seek redress through the courts.

Changes to our privacy notice

We may make changes to this privacy policy. In that case, the 'last updated' date at the bottom of this page will also change. Any changes to this privacy policy will apply to you and your data immediately.

If these changes affect how your personal data is processed, DCMS will take reasonable steps to let you know.

This notice was last updated on 19/07/2021.

Demographic questions

Are you filling in this survey as a private citizen or on behalf of an organisation?

- Private citizen
 Organisation
-

Are you willing to be contacted regarding your response to this survey?

- Yes
 No
-

Please provide your details:

Name:

Name of the organisation:

Email address:

Would you like your response to remain confidential?

- Yes
 No
-

Creating a digital identity governance framework

The governing body

1. Do you agree an existing regulator is best placed to house digital identity governance, or should a new body be created?

Characters remaining: 4952

2. Which regulator do you think should house digital identity governance?

Characters remaining: 4963

3. What is your opinion on the governance functions we have identified as being required: is anything missed or not needed, in your view?

As part of regulator and body collaboration, an important function will be to ensure interoperability to ensure integration across the UK's evolving digital infrastructure in both public and private sectors, including for example utilities. A further concern would be ensuring data integrity and preventing the sharing of data for purposes other than those of the scheme (and with appropriate data subject control and transparency).

Characters remaining: 4568

Creating a digital identity governance framework

Trust framework, standards and rules management

4. What is your opinion on the governing body owning the trust framework as outlined, and does the identity of the governing body affect your opinion?

We believe it would be appropriate for the ICO to own the trust framework as currently outlined. However we note that in order for any governing body to be effective, it will require sufficient funding and capability to deal with effective monitoring and enforcement of the framework. We believe it would be appropriate to look to the experiences of other governments as to how to engender trust in the UK government's approach. The ICO appears to us to be a trusted body as the guardian of personal data, whereas a different body may be perceived differently diminishing trust. We would like to see co-operation with the devolved governments across the UK to ensure alignment in the operation of the system regardless of location.

Characters remaining: 4269

5. Is there any other guidance that you propose could be incorporated into the trust framework?

We think it would be beneficial for the government to consider the development of an open API to better enable integration with the trust framework. This will need to be done using appropriate existing standards.

Characters remaining: 4788

6. How do we fairly represent the interests of civil society and public and private sectors when refreshing trust framework requirements?

We believe the proposal is appropriate to this aim.

Characters remaining: 4949

7. Are there any other advisory groups that should be set up in addition to those suggested?

It is important that the advisory groups include representatives from civil society.

Characters remaining: 4916

Creating a digital identity governance framework

Accreditation & certification

8. How should the government ensure that any fees do not become a barrier to entry for organisations while maintaining value for money for the taxpayer?

A small administrative fee on entry, with an annual fee linked to turnover.

Characters remaining: 4925

Creating a digital identity governance framework

Oversight/Management of organisations/schemes

9. Do you agree with this two-layered approach to oversight where oversight is provided by the governing body and scheme owners?

We suggest the government looks to the governance model for open banking in the UK, which is recognised as being world-leading.

Characters remaining: 4873

Creating a digital identity governance framework

Complaints, redress and enforcement

10. Do you agree the governing body should be an escalation point for complaints which cannot be resolved at organisational or scheme level?

Yes

Characters remaining: 4997

11. Do you think there needs to be additional redress routes for consumers using products

under the trust framework?

Yes

No

If yes, which one or more of the following?

- A governing body-led ombudsman service
- Industry-led dispute resolution mechanism (encouraged or mandated)
- Set contract terms between organisations and consumers
- Something else
- Any further comment

Provided any future development of UK GDPR contain at least the same data subject protections, we believe the existing offences are sufficient. Note that adequacy and equivalence with third country systems will be important for international interoperability, and participation in international standards may be helpful. Consumers are currently poorly served in the banking industry (e.g., with fake communications purporting to be from financial service providers), and a faster and more effective process is required for ID-related issues due to their importance. Whilst an ombudsman and mandated contractual terms may be helpful, having sufficient resources to deal with issues, and clear guidance to identity subjects, will be critical.

12. Do you see any challenges to this approach of signposting to existing redress pathways?

One potential challenge is the speed with which issues are addressed. ID-related problems need to be prioritised due to the potential for harm.

Characters remaining: 4857

13. How should we enhance the 'right to rectification' for trust framework products and services?

We agree that an operational/technical solution would be appropriate here to allow identity subjects to identify issues and correct their own data, with swift response and assistance where they are unable to do so.

Characters remaining: 4786

14. Should the governing body be granted any of the following additional enforcement powers where there is non-compliance to trust framework requirements?

- Monetary fines
- Enforced compensation payments to affected consumers
- Restricting processing and/or provision of digital identity services
- Issue reprimand notices for minor offences with persistent reprimands requiring further investigation

- Issue reprimand notices for minor offences with persistent reprimands requiring further investigation
- Any further comment

We agree that enforced compensation payments to affected identity subjects would be appropriate, in particular, among the other powers proposed. We consider it crucial that the regulator has impactful powers to both ensure compliance and provide remedies to consumers.

15. Should the governing body publish all enforcement action undertaken for transparency and consumer awareness?

Yes, provided no consumer would be harmed by the publication.

Characters remaining: 4939

Creating a digital identity governance framework

Security & Fraud

16. What framework-level fraud and security management initiatives should be put in place?

Ongoing engagement with the broader security community (including internationally) including regular workshops to remain engaged with those working on the latest developments, and an advisory board including members from across that community. We note that the US appear to be taking a lead when it comes to information security strategy, and engagement with selected US bodies may be indicated.

Characters remaining: 4605

Creating a digital identity governance framework

Inclusion

17. How else can we encourage more inclusive digital identities?

Focus on improved digital skills across the UK, and publicly accessible access points for those who do not have access to personal systems.

Characters remaining: 4861

18. What are the advantages and disadvantages with this exclusion report approach?

It is easier to measure than 'inclusion reports' and the burden is placed on the organisation rather than the regulator. However the regulator is dependent upon the organisation to deliver meaningful information.

Characters remaining: 4788

19. What would you expect the exclusion report to include?

We believe a standard should be developed with clear guidance as to what types of exclusion are covered.

Characters remaining: 4896

Enabling a legal gateway between public and private sector organisations for data checking

Protecting privacy and individuals

20. Should membership of the trust framework be a prerequisite for an organisation to make eligibility or identity checks against government-held data?

Yes, however different grades of membership should be offered depending on the degree of access. Control should remain with the identity subject as to who can access their data.

Characters remaining: 4823

21. Should a requirement to allow an alternative pathway for those who fail a digital check be set out in legislation or by the governing body in standards?

Yes, otherwise the risk of digital exclusion is heightened. We believe this is an appropriate topic for primary legislation. The digital identity scheme is voluntary, therefore an alternative should always be available.

Characters remaining: 4781

Enabling a legal gateway between public and private sector organisations for data checking

How data could be checked

22. Should disclosure be restricted to a "yes/no" answer or should we allow more detailed responses if appropriate?

This should be dependent on the identity/grade of membership of the person seeking disclosure of information. Control should remain with the identity subject.

Characters remaining: 4842

23. Would a code of practice be helpful to ensure officials and organisations understand how

23. Would a code of practice be helpful to ensure officials and organisations understand how to correctly check information?

Yes, a mandatory code of practice.

Characters remaining: 4966

24. What are the advantages or disadvantages of allowing the onward transfer of government-confirmed attributes, as set out?

This would be helpful in terms of user experience for the identity subject, and efficiency for checking organisations.

Characters remaining: 4882

Establishing the validity of digital identities and attributes

25. Would it be helpful to affirm in legislation that digital identities and digital attributes can be as valid as physical forms of identification, or traditional identity documents?

Yes, provided that there is a means to challenge the presumption in the case of error, fraud etc.

Characters remaining: 4903

Warning, pressing the proceed button will submit your response and you will not be able to submit another response through the survey.

If you do wish to change some of your answers after submitting, please contact digital-identity-consultation@dcms.gov.uk. The privacy notice associated with this email can be found [here](#).

A copy of your responses will be provided to you after you press the proceed button.