Consultation on draft legislation to support identity verification

About us:

The Local Government Association (LGA) is the national voice of local government. We are a politically led, cross-party membership organisation, representing English councils. Our role is to support, promote and improve local government, and raise national awareness of the work of councils. Our ultimate ambition is to support councils to deliver local solutions to national problems.

The Society for Innovation, Technology and Modernisation (Socitm) is a membership organisation of more than 2,500 digital leaders engaged in innovation and modernisation of public services. Established for more than 30 years, our network combines to provide a strong voice, challenge convention, and inspire change in achieving better place-based outcomes for people, businesses and communities.

The Society of Local Authority Chief Executive (Solace) is the UK's leading membership network for public sector and local government professionals. We currently represent over 1600 members across the UK and have regional branches across the country which play host to a number of events such as regional development days, skills days and networking opportunities.

Key messages:

- We agree that data sharing for identity verification will provide a benefit for individuals and households if it is implemented inclusively and with local government integrated from the earliest possible point - as both a data holder and a service provider.
- The benefits for individuals and/or households must be realised inclusively. Due consideration must be given to how citizens who do not currently hold a photographic ID or other digital footprint will be identified. Currently, the proposals do not specify what other attributes and identifiers will be used, therefore it is difficult to assess how inclusive these proposals will be or the impact of opting out.
- We agree that a real-time digital identity verification system would provide benefits for local authorities. However, we strongly contest the claim that the introduction of a data-sharing gateway would not carry cost implications for councils. This is particularly the case when considering local government as a data holder.
- The inclusion of local government and the reality of local service delivery must be considered by Government in the implementation of these proposed regulations, and the development of One Login. The stated benefit of inclusion relies on it.
- Urgent consideration must be given to the integration of health and social care bodies into the scope of this legislation. The effectiveness and local buy-in to One Login depends on it. The value to local public services in particular will depend on this.
- It is crucial that the three requirements as outlined in the Digital Economy Act are equally weighted between benefits to individuals/households and public authorities. This balance is crucial to achieving public buy-in and strengthening public trust in digital services: a stated benefit within the consultation paper.
- These proposed regulations must provide legal clarity that data sharing will only be done within the scope of identity verification. The proposed regulations, as they are currently

drafted, do not provide airtight clarity. This is crucial for building trust with those needing identity verification.

- Consideration must be given to the assurance regimes that will govern data sharing. Government must make all efforts to ensure that the burden on councils from duplicative compliance regimes is minimised, whilst still providing optimal levels of assurance between data sharers.

1. Introduction

1.1. The LGA, Socitm, and Solace are pleased to respond to this consultation on proposed regulations on data-sharing for identity verification. Our organisations represent the voice of local government and we collectively champion digital innovation across our sector. We agree that the public sector needs a national digital identity solution and that this is long overdue as a foundation for modern public services. We recognise the importance of this secondary legislation in providing the legal basis for a data-sharing gateway to facilitate the national digital identity solution, One Login.

1.2. The success and effectiveness of any national system must consider local government requirements from the outset and understand the complexity and diversity of local public services in how they are managed, delivered, and accessed. We believe the test for the legal framework and the design of the system must be whether the more complex user cases that exist in local government, including data sharing and health and social care integration, will be adequately embraced.

1.3. To ensure the lessons of previous projects, such as Verify, are learned, we are currently engaging with the Government Digital Service on the development of One Login. Along with local authorities, we are exploring how its centralised model can be enhanced to support wider public sector benefits and to build a stronger understanding centrally of the reality of local public service delivery.

1.4. Our response to this consultation reflects this reality and what is required to build an inclusive, secure, and effective data-sharing gateway for identity verification. It has been informed by engagement with the sector and the initial research carried out by Socitm with thirteen local government asks for a digital identity system. We urge the Cabinet Office to carefully consider these points to avoid legal barriers preventing the onboarding of local government to One Login.

2. Benefits for households and individuals

2.1. We agree that if implemented inclusively and with the understanding of the service delivery ecosystem at the local level, data sharing for identity verification will provide a strong benefit for individuals and/or households. In an era of increasing expectations citizens have for the efficiency and effectiveness of service delivery in a digital age, the ability to verify someone's identity in real-time without requesting evidence of a photographic ID, sometimes required in person, would produce a positive impact.

2.2. The consultation paper states throughout that these proposed regulations will support and strengthen inclusion, with additional evidence provided in the Public Sector Equality Duty Impact Assessment. However, it is difficult to assess this claim without understanding the identifiers that will be used to verify a person's identity if they do not have a photographic

ID, which we would have expected to see at the consultation stage. The estimate for those without access to appropriate photographic ID is 9% according to 2021 IFF Research commissioned by The Cabinet Office (ID that's neither in data nor the person is recognisable) and reinforced by Open Identity Exchange figure of 5.9million in 2021 (8.76%). We urge the Cabinet Office to publish these as quickly as possible to provide legal clarity for local authorities, a key objective of the proposed regulations, and to provide more detailed evidence for how these proposals will enhance inclusion.

2.3. We note in the Public Sector Equality Duty impact assessment of the proposed regulations, that young people are set to benefit the most from the introduction of these proposals. However, given that the age threshold for inclusion within the scope of these regulations is stated as 13 years old, it is crucial to state the data identifiers that will be used for those between 13 – 16 years old, especially those without a passport.

2.4. According to an Open Identity Exchange Report, of the data sets they argue would enhance and strengthen inclusion, the top two are council tax records and an NHS number. This highlights the importance of the integration of local government into an identity verification system and data sharing gateways from the earliest possible point to achieve Government's objectives. Due consideration must be given to how health and social care bodies could be included within the scope of public authorities (see section 4).

2.5. We agree that identity verification must be proportionate to the level of risk involved in the service. Any identity verification system cannot act as an unnecessary obstacle to citizens, often those most excluded, from accessing vital services.

2.6. Although beyond the scope of this consultation, the implementation of any national ID verification system requires consideration of ID verification 'off-line' options. A 'digital first, not digital only' approach would ensure that those hardest to reach and digitally excluded would share the benefit these data-sharing regulations promise and non-digital options are equally as convenient for citizens. Practical examples include a phone ID verification using the same data-sharing gateway or a QR code of a verification check that someone can present when accessing services. Again, we note that younger people were shown to positively benefit from the implementation of these proposed regulations. However, if identity verification is not implemented in a way to also allows for offline options, this may negatively impact older people and other groups that are not 'digital natives'.

2.7. It is unclear whether there will be a means for citizen recourse if an ID check fails. This may be due to incorrect data provided by the citizen but could also include incorrect data held by the public authorities. Government must consider the recourse possible for citizens in instances of failed ID checks, and a mechanism is put in place to address and resolve them.

2.8. Paragraph 34 states:
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.

We welcome this, however as it is currently drafted, it reads as these fraudulent checks will only be done at the outset when an identity is being verified. A principle enshrined in One

Login is that identity verification will be done once to minimise the burden on the citizen. Due consideration therefore must be given to how ongoing checks and balances will be undertaken to ensure that an identity, once verified, isn't being used fraudulently, for example in the case of a coercive controlling relationship.

3. *Benefits for local government*

3.1. As a service provider, the ability to verify an identity digitally could serve as a significant productivity gain for councils if local government is integrated effectively into the design and delivery of the national system and if the implementation is properly resourced. It could serve to strengthen the relationship between the council as a service provider and residents with a more seamless user experience of public services. Crucially, in the context of reducing resources for local government, this could save resources and capacity for councils to focus on delivering public services.

3.2. Local government handles an enormous amount of citizen data. It is used for many functions, such as children's services, social care, democracy, housing, and welfare. Sharing data across tiers of government can bolster digitisation efforts, improve the user experience and optimise costs. If their role as a data holder is properly resourced, local government inputs could contribute significantly to ensuring that any identity verification or data sharing is done so in the most inclusive way possible, removing barriers for those without photographic IDs.

3.3. However, we challenge the claim that these regulations will not have any financial implications for local authorities, especially as a data holder, and would urge Government to provide evidence that supports this claim. According to the New Burdens Doctrine:

It is not acceptable to argue there is no burden because local authorities can choose not to use the powers. Where central government goes to the trouble of developing or legislating for a specific discretionary measure, it must be on the basis that authorities are expected to make some use of it, creating potential costs for authorities, and potential pressure on council tax.

The successful implementation of this legislation and One Login depends on the participation of local government, both as data holders and service providers. This will require capacity and resources on behalf of local authorities that need to be taken into consideration. For example, in the technologies required to enable the intended data flows, the development of APIs will be required to ensure that data can be exchanged in a way that is interoperable with other public sector systems. Given the reliance on private sector suppliers for case management systems, these interoperability aspects could prove expensive if all local authorities are charged separately for the integration of data. If it is too costly for local authorities to participate in One Login, they will not do so. Without due consideration of the costs, smaller councils could be deterred from participating to the detriment of their local communities and the inclusivity of One Login.

3.4. The drafting of business cases, data protection impact assessments, and information sharing agreements are onerous tasks. We would strongly urge the Cabinet Office to provide draft DPIAs and business cases that local authorities can then adapt. Information Sharing Agreements must be co-created with local government, such as through a local

government sector-led working group, which can then be adapted for different council contexts if the council chooses to participate.

3.5. Due consideration must be given to whether the introduction of data sharing will increase a council's risk and liability in the handling of data, which in turn could increase insurance premiums. We urge the Cabinet Office to consult insurance specialists to clarify the impacts on costs. It's crucial that information sharing agreements are risk assessed and are aligned with the specific local authority's risk appetite.

3.6. Sufficient investment in local government is needed to ensure that councils have the necessary resources, capacity, and data foundations in place to engage in data-sharing developments. Low budgets and underinvestment have hampered efforts to ensure that the right people and technology are in place. Additionally, we have seen good initiatives, supported by central government, discontinued such as the Integrated Public Sector Vocabulary.

3.7. Paragraph 46 states:
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".

It is unclear how these proposals will positively impact the government's 'levelling up' agenda, and more clarity is required. If there is not more support provided to councils to strengthen their data foundations, the councils with the highest degrees of financial certainty will be less likely to be in a position to prepare for the integration into One Login.

3.8. Paragraph 38 states:

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 act 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.

More clarification is required as to how these proposed regulations will or will not be used to address fraud. The regulations state the benefits as addressing fraudulent use of services, then later state they are not intended to be used as a mechanism to act in a fraud offence. If local authorities are duty-bound to take their own decisions on fraud management, there appears to be a contradiction in the intended usage of the data, potentially also having implications on minimisation and retention. More clarity is required.

3.9. It is crucial Government recognises the service delivery ecosystems that exist at the local level, both with the commissioning of services and with the delivery of social care (see part 4). Due consideration must be given to how these proposed regulations would impact local government's engagement with the voluntary and community sector, given the extent of commissioned services – normally with the most vulnerable in society, and private sector suppliers. The LGA, Solace, and Socitm are committed to supporting the government in whatever way we can to capture this complexity and strengthen the effectiveness of identity verification.

4. Exclusion of health and social care bodies

4.1. We are concerned about the exclusion of health and social care bodies from the scope of this legislation. 'In particular, we are concerned about the impact this will have on the 152 councils in England who deliver social care, and what this will mean for integration into a national identity verification system. There is a strategic discussion required between the Cabinet Office, DHSC, and NHS England on whether the NHS is considered a public authority in the One Login system, or whether it is preferred that they continue to use the NHS app. If health and social care are not integrated, this could entrench and complicate an already fragmented system by its exclusion, and may disincentivise the use of One Login once developed in those 152 councils. Given that social care is delivered at the local level by unitary or county councils, the failure to integrate social care will negatively impact all communities in England.

4.2. We understand the complexities of health and social care data, and strongly agree that any health or social care data sharing is done so with patient and client consent enshrined. It is clearly stated in the consultation paper that a public authority can be a service provider and/or a data holder. Local government will be both. Due consideration must be given to what excludes health and social care bodies from being a requester of identity verification without necessarily being a data holder.

4.3. The absence of health and social care bodies from the consultation is not clarified other than a reference to them not being included in the scope of the Digital Economy Act 2017 for data-sharing purposes. The Code of Practice to the Digital Economy Act states in paragraph 41:

Arrangements for information sharing under this Code of Practice therefore should not include health and adult social care bodies in England or any non-devolved activities. Until the recommendations made by the National Data Guardian's Review of Data Security, Consent and Opt-outs have been implemented and there has been public consultation, including with appropriate representative health bodies, adult health and social care bodies in England and for non-devolved activities will not be added to the Schedules.

This omission also results in the NHS app, with over 40 million verified users, unable to be used as a source of data for verification of identity.

4.4. Whilst the National Data Guardian review is now complete, there does not appear to have been a consultation on including health and social care records for information sharing under section 35. Therefore, without consultation, it is assumed that the current identity verification checks for social care applications to local authorities will continue on the current basis. If this exclusion is not addressed, social care services in councils will not be able to benefit from these proposed regulations and the subsequent introduction of One Login.

5. *Trust between citizen and the government*

5.1. Given the political contentions around the introduction of a digital identity system, trust and transparency are of paramount importance to the implementation of these regulations. Local government is the front line of government service delivery for communities and therefore will bear the brunt and burden of the negative impacts caused by any loss of trust.

5.2. Public trust in the ethical use of personal data is low. A poll by the Open Data Institute and YouGov (2019) found that only 31 percent of people said they would trust their local authority to use personal data about them ethically – and 30 percent replied in the same way about central government. When asked which type of data they would be comfortable sharing with their council in exchange for a public service – and the kinds of data they would be comfortable with their council collecting – far fewer than 50 percent said they would be happy with any of the scenarios presented (except for air quality data). Local government is beginning to consider data ethics in the digital transformation of services to address this distrust. An example of which is Camden Council's 'charter', which enshrines the citizen's right to define what ethical data processes look like. However, these require staff time and resources to develop and implement.

5.3. Equally, central government departments need to be transparent about avoiding racial, gender, and other bias in the data that is made available for identity verification and the way in which such data is used, secured and protected from cyber and other risks.

5.4. We believe that this legal framework should be flexible, that allows credentials to be owned by an individual and shared to enable identity verification for access to a wide variety of public services, including ones delivered at the local level.

5.5. We note that Data Protection Impact Assessments (DPIA) were carried out as part of the Government Digital Service's One Login development. We are unable to consider the data protection aspects of this legislation without understanding what the identified impacts are.

5.6. We have concerns that there is legal ambiguity in how the proposed regulations are currently drafted. Ensuring that the secondary legislation provides airtight legal clarity that data sharing will only be done for identity verification is crucial. This clarity will benefit the citizen and trust levels and will also protect local authorities from relying on Information Sharing Agreements to clarify, which would incur an additional burden of liability.

5.7. In the consultation paper, paragraph 43 states:

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 in savings across departments through avoided costs and duplicate digital identity systems; and more and better-quality insights for Ministers to inform policy.

It is unclear what insights will be gleaned from these proposals if the regulations only allow for data sharing in the context of identity verification. More clarity is required to prevent legal ambiguity and to promote trust. We strongly support the Register of Information Sharing Agreements developed under the Digital Economy Act and would like to see the wider adoption of this register to strengthen transparency.

5.8. A crucial aspect of building citizen trust is data security. A foundation of data security is ensuring that data in transit is minimised. We welcome the proposed regulations commitment to minimising the data shared between public authorities beyond the result of the identity verification check. However, without the proposed regulations clarifying what 'other attributes' and identifiers will be used in the processing of data to verify one's identity

without a photographic ID (paragraph 26), it is difficult to assess the extent and scope of data in transit and the subsequent information security aspects.

6. Trust between public authorities

6.1. Trust between public authorities is vital to facilitate data sharing for identity verification. Assurance is an important foundation of any data-sharing agreement so that public authorities involved trust the integrity of the data used to verify a service users' identity, and the processes used to do so have data security principles enshrined.

6.2. In the proposed regulations, it is unclear as to what assurance mechanism will be used to strengthen this trust between public authorities and how assurance regimes will integrate with others. These details will be borne out of the Information Sharing Agreements, however at this early stage, we urge Government to strategically engage with other departments currently considering assurance frameworks that have information security aspects, such as the sector-specific roll out of the National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF). The Department for Levelling Up, Housing and Communities are currently developing the Local Government Cyber Assessment Framework (LGCAF). Due regard must be given to integrating assurance around these proposals as possible to avoid multiple duplicative compliance regimes falling to local government. If done in an integrated way, this could also potentially serve to minimise any new burden costs.

Key contacts:

LGA: Jenny McEneaney
Senior Improvement Policy Adviser: Cyber, Digital, and Technology
jenny.mceneaney@local.gov.uk

Socitm: Martin Ferguson
Director of Policy & Research
martin.ferguson@socitm.net

Solace: Alison McKenzie-Folan
Spokesperson for Digital Leadership and Chief Executive of Wigan Council
a.mckenzie-folan@wigan.gov.uk