The Information Commissioner's Response to the Government's Digital Identity and Attributes Consultation

About the ICO

The Information Commissioner has responsibility for promoting and enforcing the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA), the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR) and the Privacy and Electronic Communications Regulations 2003 (PECR). She is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

Introduction

The Information Commissioner's Office (ICO) welcomes the opportunity to respond to the government's Digital Identity and Attributes Consultation. This response builds upon our position paper on the UK Government's proposal for a trusted digital identity system published on 22 April 2021. In this paper we expressed our support for the introduction of a UK digital identity and attribute framework. We noted that such an overarching framework can bring many economic as well as privacy benefits over reliance on paper identity records. In addition, we acknowledged the government's proposed framework and accompanying governance regime also has the potential to bring individual protections and trust to the existing digital identity ecosystem. We were also clear, however, that development of the framework must be based on risk assessment and in accordance with data protection law.

Having considered the consultation document, we are pleased to see the importance being placed on privacy and transparency in the design and structure of the government's proposal. In particular we welcome the inclusion of a comprehensive governance regime with a focus on individual redress, enforcement and collaboration with other regulators. We also welcome the government's acknowledgment of the importance of data protection rules whilst enabling a legal gateway between public and private sector organisations for data checking.

This response follows the structure of the consultation document, first providing comment on the government's overall approach to this proposal and then on the three sections of the consultation document: creating a digital identity governance framework; enabling a legal gateway between public and private sector organisations for data checking; and establishing the validity of digital identities and attributes.

Government approach

We welcome the data protection by design and default approach taken by the government on this proposal. We are also pleased to have been consulted throughout the development of the trust framework and accompanying governance regime.

We recognise and welcome that the government's proposal does not take a centralised approach to digital identity and attribute verification. The proposed distributed and federated approach mitigates many of the core privacy risks that would emerge from a centralised scheme, however, there is still detail missing as to how the system will work in practice. Although we appreciate much of this detail is deliberately being left to those organisations and schemes who will become members of the trust framework, it would be desirable for the government to consider publishing data flow models and user case examples to show how an individual's data will move through the ecosystem. This would enable better understanding for individuals, regulators and other interested parties. Mapping and identifying data flows has an important impact on transparency. People need to be able to understand who is processing their data at what stage and for what purpose so they can have trust in the system. Similarly, it is important for the government and the ICO to be clear on controllership relationships under this proposal. We would welcome a commitment from the government to publish such information at their earliest convenience.

In our position paper of April 2021, we requested the government carry out an overarching data protection impact assessment (DPIA) for the proposal. This is important to ensure risks have been appropriately articulated and mitigated against. The consultation document does not effectively articulate the risks of the proposal, especially in relation to security. We would expect to see these as part of a DPIA. The government have since committed to publishing this alongside the beta version of the trust framework. We look forward to considering the DPIA at this time.

Creating a digital identity governance framework

We welcome the government's creation of a clear governance framework for digital identity. We are pleased to see well-defined roles, responsibilities as well as rules, standards and an independent oversight body, all of which are critical to providing trust and confidence to individuals.

The governing body

We welcome the government's suggestion of housing the body within one regulator to undertake the functions outlined in the consultation paper. Multiple regulators can sometimes cause problems relating to regulatory overlap and from our experience it can sometimes be difficult for the public to navigate their way to appropriate redress if there are a number of bodies that are seen as operating in the same sphere or sector. A single body will also enable clear guidance and support for those organisations and schemes covered by the framework. We recognise the benefits of housing these functions with an existing regulator for these reasons as well as the economic benefits highlighted in the paper.

The requirement for the governing body to publish reports on its progress and actions is also welcome. We would also recommend to the government to designate the governing body as a public authority for the purposes of FOIA. Transparency is intrinsically linked to trust and we believe it very important that the governing body is subject to FOIA for this reason. Similarly, it is important that the governing body is subject to the same levels of scrutiny and accountability as other regulators operating in this sphere.

In particular, we welcome the inclusion of the requirement for the governing body to collaborate with other regulators. This is crucial for ensuring the success of the governance framework. From a data protection perspective, there are areas where the ICO's regulatory responsibilities will likely need to dovetail carefully with those of the governing body – in particular with regards to security, enforcement, complaints and redress, as well as collaboration when updating and refreshing the trust framework. We look forward to learning more about how this will work in practice once the government have confirmed which existing regulator the governing body role will sit with.

The ICO can also draw from its current experience of engaging with Ofcom and the Competition Markets Authority in the Digital Regulation Co-operation Forum.

Complaints, redress and enforcement

The government sets out in the consultation document their proposal for the governing body to act as an escalation point for individual complaints where they have not been resolved through trust framework organisations or schemes, where applicable. This escalation point is of utmost importance. Although it is clearly important for trust framework organisations to have their own procedures for dealing with complaints and rectifying inaccurate data, in an ecosystem such as this where there can be multiple controllers, it is important for individuals to be able to get their data corrected throughout the wider ecosystem. The governing body should have a role to play in ensuring this happens.

We welcome the government's commitment to not making any new offences relating to digital identity. We believe this is the right approach and agree that in practice the vast majority of breaches are likely to also fall under data protection legislation. A new offence would likely cause confusion in this respect. It is, however, important to be clear that data protection law relates primarily to controllers, we would ask government to consider whether there are other potential harms that could arise other than by controllers. Such actions could fall outside of data protection law.

We recognise the government's acknowledgement that the complaints process for digital identity will need to have a clear relationship to the ICO's existing data protection complaints process. Given the volume of data protection complaints currently received by the ICO, it will be important to model the possible impact on our complaints function and how this will be resourced, if digital identity complaints significantly increase intake beyond current ICO baseline. In 2020-21 the ICO received 36,607 DP cases. It will also be important that the ICO is able to meet expectations of the public in terms of individual case resolution. We look forward to discussing this further with the government once the governing body regulator has been confirmed.

The government sets out a number of options for redress to be made available outside the courts whereby individuals can seek compensation, through a claim, for a harm that has been inflicted upon them by one of the actors in the digital identity system. Given the tangible nature of the harms that could appear in the system, particularly financial impacts, the ICO welcomes the proposal and different options. We want to understand the possible benefits, impacts and costs of the different models in more detail before providing a view on what may be the preferable option.

Whilst we are supportive, we note that no such mechanism exists for individuals who have suffered harm through other data protection

breaches, therefore specific justification for the digital identity context should be provided.

The government sets out a number of potential enforcement powers that could be available to the governing body if it finds that organisations or schemes are not complying with the rules of the trust framework. We welcome the ability for the governing body to have certain powers, such as the ability to issue warnings and expel or suspend members from the trust framework, however, it is important that these powers do not duplicate powers that are already available to the ICO for the same breaches. Some of these powers will be unique to the body, such as expulsion. But for some of the broader powers, measures may need to be in place to manage the risks of unfair or duplicated action- for example, an organisation being given two penalty notices for the same or very similar breach of data protection law – one by the ICO for the data protection breach and one by the governing body for the trust framework breach.

The consultation document suggests that an appropriate balance may be escalation to other regulators, such as the ICO. We believe this would be a more effective solution in order to avoid regulatory overlap in certain circumstances. The resource impact of any escalation would also need to be considered. There are also learnings from how the ICO currently manages the system for data breaches, alongside the Financial Conduct Authority's regulatory regime for breaches in that sector.

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

The government sets out in the consultation document the proposal to create a legal gateway to create a power for government departments and agencies to confirm personal data with organisations for eligibility, identity or validation checking purposes. We recognise the legal clarity this will bring to government departments and agencies and welcome the confirmation that this will provide a power to share data for this purpose rather than place a legal obligation for them to do so. This allows departments and agencies to use their judgement as to whether it is appropriate to share their data and if so, what data is appropriate to share.

Lawful basis and special category data

The government rightly acknowledges that as well as a legal power to share, government departments (and the organisations making the

checks) will still need to have a lawful basis for processing personal data under UK GDPR. Although controllers will be responsible for deciding on the most appropriate lawful basis (or bases) based on their context specific processing, we would ask the government to give further consideration as to what lawful basis (or bases) would likely be most appropriate for this purpose and provide advice to departments and organisations accordingly. We are happy to discuss this with the government and advise where helpful.

As well as a lawful basis, the government should carefully consider the desirability, impacts and risks of allowing special category data (such as health, genetic, biometric or those revealing ethnicity or religious beliefs) and data relating to criminal convictions and offences to be shared for eligibility, identity or validation purposes. This is particularly the case in scenarios where an individual may have little choice or outcomes could have a significant effect on them. The sharing of such data would require additional safeguards and it is likely that further legislative change would be required to enable sharing for these purposes.

Membership of the trust framework as a prerequisite

The government asks whether membership of the trust framework should be a prerequisite for an organisation to make eligibility or identity checks against government-held data. We believe that it should be. Although organisations will be subject to UK GDPR protections regardless of whether they are members of the trust framework or not, membership is extremely important in ensuring specific safeguards and standards to complement and enhance data protection.

We agree with the government's assertion that there needs to be clear governance around any new legal gateway with industry or there is a risk of damaging public trust. Making the trust framework a prerequisite provides that governance mechanism whilst also providing assurance for government departments and agencies that data will be protected appropriately following a data share. In addition, membership provides additional assurance and safeguards for individuals. This is important for ensuring trust and confidence in the system.

Requirement to allow an alternative pathway and restrictions to automated processing

We welcome the government's assertion that a service should not be denied to individuals solely on the outcome of a digital government check. There are many situations where individuals may not have government held data, for example, vulnerable adults, children, those with protected identities or those who do not need to or indeed choose not to have a

government identity. It is essential that alternative methods are available in these circumstances.

In addition, it is important for the government to consider how UK GDPR Article 22 may apply to the processing for eligibility, identity or validation checking purposes. Article 22 applies to solely automated decision-making that has a legal or similarly significant effect on the individual. Whilst much processing for this purpose is unlikely to result in a legal or similarly significant effect, there are also likely to be situations where it does. Controllers can only carry out this type of processing where it is necessary for the entry into the performance of a contract, authorised by domestic law applicable to the controller or based on the individual's explicit consent. Where Article 22 applies, individuals have the right to ask for a review of any automated decisions made so there must be an alternative method available.

Data minimisation

The government asks in the consultation document whether disclosure should be restricted to a yes/no answer or whether a more detailed response should be allowed if appropriate. One of the cornerstones of data protection law is data minimisation (UK GDPR Article 5 1.(c)). This means that controllers must ensure the personal data they process is adequate, relevant and limited to what is necessary for the purpose for which they are processing. In this context, it means that organisations should only process data that is necessary to verify an individual's identity or attribute. In most cases a yes/no answer is likely to be adequate for checking purposes and no further additional information would be required. However, we recognise that there will be scenarios where further information is necessary and proportionate. Data protection law in general, and the principle of data minimisation specifically, do not pose a barrier to such data sharing. We therefore support the government's starting position that checks are best made via yes/no attribute checking, but that further personal data can be shared in accordance with data protection law where the necessity of sharing that data can be justified. Consideration of this question may also need to form part of data protection impact assessments.

Codes of practice

We welcome the government's suggestion of a code of practice for digital identity to help ensure officials and organisations understand how to correctly check information. The Information Commissioner has produced a statutory Code of Practice for Data Sharing under section 121 of the DPA. This is a practical guide for organisations about how to share

personal data in compliance with data protection law. As the government notes in the consultation paper, the powers to share information under Part 5 of the Digital Economy Act 2017 (DEA) are supplemented by codes of practice. Under the DEA, these codes of practice must be consistent with the Information Commissioner's data sharing code of practice. We suggest that a code of practice for digital identity also be consistent with the Information Commissioner's data sharing code in the same way. This will ensure that the various codes dovetail appropriately and avoid confusion.

Onward transfer of government–confirmed attributes

The government asks in the consultation document about allowing the onward transfer of government-confirmed attributes. It is unclear from the document in what circumstances onward transfer would be allowed. It would be helpful for the government to confirm whether this would be restricted to organisations under the trust framework and also whether it would be restricted for the purposes of eligibility, identity or validation.

In our experience, failure to limit the purposes for which organisations process personal data poses a risk to individuals. People have a reasonable expectation that organisations will use their data for the purpose(s) they are told about at the outset. It would significantly undermine the public's trust in the framework if organisations use data obtained from the government in a way they would not expect. In addition, processing data collected for one purpose for another incompatible purpose (where an exemption does not apply) is a breach of UK GDPR. Even where purposes are in theory limited, if onward transfer of government- confirmed attributes was allowed beyond the governance regime of the trust framework then there is a danger that individuals will lose visibility of how and by whom data is being used and therefore be rendered unable to exercise their information rights.

Establishing the validity of digital identities and attributes

We welcome the government's proposal to affirm in legislation that digital identities and digital attributes can be as valid as physical forms of identification, or traditional identity documents. It is sometimes tempting for organisations to see the status quo as the best way to avoid risks and this can certainly be the case when it comes to privacy. The ICO is keen to encourage innovation and embrace new data technologies to improve the services offered to the public by both commercial and public sector providers. We see the many benefits that digital identity and attribute verification can bring. These include privacy benefits over paper identity records, such as individuals only needing to provide data that is necessary

for the check, and better protection against loss, damage or theft. Affirming the validity of digital identities and attributes in legislation should help to give organisations and individuals further confidence in using them.

Conclusion

The government's digital identity and attributes consultation outlines proposals to create a digital identity governance framework, enable a legal gateway between public and private sector organisations for data checking and establishing the validity of digital identities and attributes. We welcome the government's continued commitment to taking a data protection by design and default approach to these proposals. We hope the comments provided in this paper are useful to the government. We are pleased to have been consulted throughout the development of these proposals and look forward to providing input in an advisory and regulatory capacity as it further develops.