The Information Commissioner's position paper on the UK Government's proposal for a trusted digital identity system

22 April 2021

Executive summary

In February 2021, the UK Government published their policy paper for a UK digital identity and attributes trust framework, proposing the introduction of a trusted digital identity system. The ICO understands that the framework is currently in alpha form, to allow for changes as proposals develop. Their policy paper gives example use cases for digital identities within the government framework, such as proving who you are when opening a bank account or starting a new job. This position paper sets out the Information Commissioner's positions in response to these proposals, in line with the data protection by design and default principle.

Driven by the opportunities and challenges of the digital economy and public services, digital identity systems are now becoming more common, particularly due to the COVID-19 pandemic. The public need safe and secure ways to establish their identity in light of the reality of how digital services work in their daily lives. These systems also need to recognise the risks of fraud and security that exist in our current situation, including the continued reliance on paper records.

The implementation of digital identity systems in a significant number of comparable countries around the world highlights that these systems can be developed to ensure privacy for the public.[1] The Information Commissioner sees many benefits to Government's digital identity proposals, such as:

- creating more straightforward access to services;
- promoting efficiency savings; and
- providing a framework that gives assurance to individuals and providers.

The proposed model takes a distributed and federated approach.[2] This approach mitigates many of the privacy risks that would emerge from a

[1] See Annex for further details.

[2] A distributed and federated approach means data is not held centrally but is distributed amongst various controllers in the system. This allows interoperability, and only essential

centralised scheme, such as unwarranted intrusion or lack of autonomy. However, a system of this size and complexity still has underlying risks. We therefore want to support Government to get the privacy considerations right so there is trust and confidence in the system, whilst also protecting the public's information rights.

In this paper, the Commissioner welcomes the data protection by design and default approach Government is taking. She also highlights relevant and practical requirements of data protection law that must be implemented and the importance of robust governance and clear accountability. The paper also provides international models of digital identity verification. The paper then outlines a number of key expectations for a trusted digital identity system, highlighting the importance of:

- a user-centric approach;
- having clear responsibilities and liabilities;
- accuracy;
- purpose limitation;
- considering automated processing; and
- mitigating specific risks for children.

The Commissioner welcomes continued engagement with Government on their proposals and looks forward to providing input in an advisory and regulatory capacity as they develop.

Purpose

This document sets out positions in response to the UK Government's (Government) alpha proposal for a trusted digital identity and attribute framework and its development in line with the data protection by design and default principle.

Audience

The Information Commissioner's Office (ICO) has primarily developed the positions outlined below for Government policy makers working on the introduction of a digital identity system. We have a strong working relationship with the Department for Culture, Media and Sport (DCMS) on digital identity and this document is part of our ongoing work to provide

and minimised information sharing between de-centrally organised controllers, providing increased control to individuals and increased security to their data.

independent advice. In addition, this paper may be of interest to organisations involved in the digital identity ecosystem, that need to understand how to apply information rights and data protection by design and default approaches to the development, deployment and monitoring of digital identity systems. This includes policy professionals, design teams, monitoring bodies and risk management professionals – including, but not limited to, those working in privacy and data protection, information security, compliance and operational risk.

Scope

We are providing this paper to give regulatory advice and guidance to DCMS and the wider stakeholder community regarding the proposed trusted digital identity system[3] and associated activities. We are an independent, pragmatic regulator that upholds information rights in the digital age. Elizabeth Denham, the Information Commissioner, is committed to privacy and innovation working hand in hand in today's evolving economy. It is essential that organisations build privacy and data protection into the development and secure use of digital identity systems. This, in turn, enables greater trust and confidence in their use.

Legislation

We limit the legislation we cover in this position paper to those that fall within our regulatory remit, specifically data protection law and the eIDAS Regulation.[4] For clarity, where we make reference to data protection law, this refers to the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

Terminology

For the purposes of this paper, we broadly mirror the terminology in the UK Digital Identity and Attributes Trust Framework.

DCMS describe the framework as:

"A trust framework is a set of rules and standards which organisations agree to follow. If an organisation is part of the digital identity trust

[3] https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework

[4] For further information on the legislation that the ICO regulates, please refer to the legislation we cover section of the ICO's website.

framework then you know they follow agreed requirements which safeguard your data and protect your privacy.

"The UK digital identity and attributes trust framework sets out requirements so that organisations know what 'good' identity verification looks like."

The framework defines digital identity as:

"…a digital representation of a person. It enables them to prove who they are during interactions and transactions. They can use it online or in person."

And an attribute as:

"Attributes are pieces of information that describe something about a person or an organisation. You can use a combination of attributes to create a digital identity. You must 'bind' an attribute to a person before you can do this."

COVID-19 certification

Although there are clearly parallels and points of relevance, this paper does not cover the potential use of COVID-19 certification, digitally or otherwise. We are inputting into reviews separately on this issue by the UK Government and devolved administrations. We published a blog on this topic on 26 March[5]. A data protection by design approach is essential for both areas.

Overarching approach to the introduction of a digital identity system

We responded to the 2019 DCMS digital identity consultation outlining key data protection considerations in the development of government policy regarding digital identity. Following this consultation, Government developed their work in this area and recently published their identity and attributes trust framework. Separately, we also engaged with the Scottish

[5] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/data-protection-law-can-help-create-public-trust-and-confidence-around-covid-status-certification-schemes/

Government on the development of their Digital Identity Scotland (DIS) programme, providing feedback through the DIS Expert Group.[6]

We welcome Government's continued engagement with us on this project. We are keen to provide input in an independent advisory and regulatory capacity as it develops. We also look forward to consultation on future legislation and data protection impact assessments (DPIAs) where useful or as required by law.

The public need safe and secure ways to establish their identity, given the reality of how digital services work in our daily lives. These systems must also recognise the risks of fraud and security that exist in our current situation, including a continued reliance on paper records. The COVID-19 pandemic further highlights these challenges. There is a valid case for a new digital system as a privacy friendly and secure alternative to our current systems that still often rely on paper documents.

As well as economic benefits, there are likely to be privacy benefits because of the reduced reliance on paper identity records, which can be lost, damaged or stolen. In addition, we appreciate the added protections that an overarching trust framework and accompanying governance regime can bring. However, those designing the framework must consider the privacy risks at key stages of development and in accordance with data protection law. We welcome Government's commitment to a data protection by design and default approach. Good data protection practice helps to inspire public trust and confidence and enables an effective digital identity regime.

Previous Information Commissioners responded to proposals for government-issued identity cards, most notably in the early 2000s. We raised concerns about the scope and purpose of a centralised scheme. As noted above, digital identity systems have come of age, with successful use cases in other jurisdictions using alternative approaches.[7]

We recognise and welcome that the Government's proposed approach for a trust framework does not take a centralised approach. The proposed distributed and federated approach mitigates many of the core privacy risks that would emerge from a centralised scheme.

International models of digital identity verification

[6] https://www.gov.scot/policies/digital/digital-identity-scotland/

[7] See Annex for further details.

We acknowledge that a variety of international schemes and frameworks have or are implementing digital identity verification. These are at varying stages of maturity and have differing levels of data protection underpinning them. They also have different aims and connections with public information systems, such as national identity cards or public service entitlement cards.

It is important for Government to keep abreast of international developments, to ensure any digital identity schemes and frameworks adopt benefits from the findings and learnings of other countries' initiatives. This includes systems with effective privacy safeguards that achieved strong public take up and engagement. See Annex for further detail of international models of digital identity verification.

Compliance expectations

Accountability

Accountability is a key feature of the UK GDPR and requires organisations to actively demonstrate their compliance with, and commitment to, data protection legislation. This may involve undertaking DPIAs and embedding data protection by design and default into their systems and processes.

Engaging accountability throughout the digital identity system is a positive opportunity. It enables organisations to demonstrate how they respect the public's data protection rights by complying with the law, which helps to develop and sustain people's trust. Therefore, when developing new or innovative methods of processing personal data, it is crucial that organisations demonstrate their accountability to ensure that the public trust how organisations use their data.

Certain organisations must carry out DPIAs, as part of the accountability requirements. The DCMS trust framework requires organisations to carry out DPIAs for identity and attribute services. It is likely that, given the nature and volume of the data it involves, any controller substantively involved in accommodating digital identity verification would need to carry out a DPIA by law. It may also require an ICO review.

We work closely with Government to ensure organisations process personal data in accordance with the law. This includes any legislation they bring forward related to digital identity, as part of any formal consultation from the UK Government under Article 36(4) of UK GDPR.

Governance

Clear governance frameworks, with well-defined roles and responsibilities as well as rules and standards that a system of independent oversight and enforcement effectively upholds, are critical to the proposed system's success. This can also support compliance with data protection requirements. We understand that the full details of these mechanisms are not yet available, including the introduction of an oversight body and its relationship to us. We look forward to considering these matters further when more detail is available. Whatever model is agreed upon, the oversight of digital identity systems and the regulation of data protection will need to be appropriately joined up. This will help ensure there is no duplication of effort as well as guaranteeing a clear pathway for individuals' redress and regulatory clarity for service providers, along with all other parties within the digital identity ecosystem.

User-centric approach

We welcome the introduction of a comprehensive government approach that facilitates fair and proportionate data sharing and provides a shared framework and set of standards to which all parties have to adhere. In particular, we welcome UK government's support for a user-centric approach that provides controls over data release and gives individuals choice and agency about the disclosure of their personal data, as required by data protection legislation.[8] Such a principle provides a number of advantages in safeguarding privacy.

There are particular risks of harm associated with a single entity or group of entities processing all user data in an identity management system, depending on the specific context of the processing and how it is undertaken. For example, the consequences of a personal data breach could be significant, leading to:

- financial harm or emotional distrust;
- misuse of personal information; or
- loss of trust.

Whilst, the DCMS trust framework explicitly prohibits creating aggregate datasets, the potential for correlation of an individual's activities across multiple online services would also need addressing.

[8] See UK GDPR articles 12-22.

We therefore highlight the importance of concepts such as federated identity management, attribute-based credentials and tokenisation. Coupled with on-device processing, this can reduce the likelihood and severity of potential risks and harms, such as:

- misuse of personal information;
- loss of trust or unwarranted intrusion; and
- decrease in cost (both in terms of implementation and compliance).

Such approaches can also align with the principles of data protection by design and by default, for example by facilitating individual rights and integrating necessary safeguards into the processing.

International best practice highlights the need to take a user-centred approach, as seen in British Columbia, Denmark and Norway to ensure users maintain control over how organisations use their data.

Controllership and data sharing

In its current form of an early-stage prototype, the Government's trust framework does not set out clear responsibilities or liabilities for certified organisations involved in a digital identity system. The UK GDPR distinguishes between controllers, joint controllers and processors of personal data. They have differing legal responsibilities and it is essential in a trust framework, where many different organisations are responsible for certain aspects of data processing, that all parties understand their responsibilities and liabilities. This clarity also provides effective accountability and transparency, a legal requirement in data protection law, and in turn increases the trust and confidence of the public. We explain the importance of accountability in more detail below.

Mapping data flows between different systems, controllers, processors and the public is equally as important to understanding controllership responsibilities. Mapping and identifying data flows has an important impact on transparency for individuals. 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 and provide their informed consent where appropriate. Similarly, understanding data flows is essential for important redress mechanisms and allowing individuals to exercise their data protection rights.

We appreciate that Government's trust framework is currently in alpha form, has only recently been consulted on and is subject to change. However, we recommend that Government requires mapping and publishes potential data flows and controllership relationships at the earliest opportunity, ensuring appropriate consultation and review as the project develops. This could be part of an overarching privacy impact assessment or at scheme level, as outlined above.

It is important for Government to also fully consider other forms of personal data, not directly used for digital identity verification, which the process may create. One example is analytics data, which organisations create to look at who is using digital identity services for what purpose. Organisations need to account for this data as part of a mapping process and the trust framework needs to consider and protect it appropriately.

Organisations operating within the trust framework should take account of the provisions of the ICO’s Data Sharing Code of Practice. This ensures any sharing of personal data they undertake is compliant with data protection legislation.

Accuracy of data

Robust arrangements should be in place to ensure the underlying data in any system within the framework is accurate, up-to-date and relevant. Incorrect or out of date information could lead to members of the public being unfairly refused services. Consideration needs to be given to the practical aspects relating to accuracy, such as how data is rectified in a timely manner throughout a system or across the wider ecosystem where there are multiple organisations that may hold incorrect data. The trust framework should also ensure they have regular audits.

It is key that appropriate, easy to access and simple to use redress mechanisms are in place for members of the public whose data is inaccurate. Alongside the legal requirement on each controller it is additionally important, as good practice, for Government to consider how the trust framework requirements and governance can enable individuals to get their data corrected throughout the wider ecosystem, rather than having to contact individual controllers. We consider this to be important in respect of ensuring the public are not denied access to services and they have trust and confidence in the system.

Purpose limitation

We welcome the Government’s trust framework reference to identity service providers not using digital identity data for profiling or marketing. It is important that **all** organisations involved in the framework, including Government and other public bodies, have a clear dividing line between the processing of data for digital identity verification purposes and all other purposes. Profiling data collected for digital identity purposes, in particular, could be intrusive and involve organisations evaluating data both within the system and related to the system (such as how often and where they made an identity check) to build a picture of an individual. It is important that no organisations use data they collect for digital identity purposes for wider profiling.

This is not to say that individuals should need to provide their data for digital identity purposes when it has already been provided for other compatible purposes. It means that organisations should not use the data a person provides specifically for digital identity verification for other purposes except where allowed by law or with an individual's permission.

In our experience, failure to limit the purposes for which organisations collect 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 people's data in a way they would not expect. This could be the case both with private sector organisations and within Government. In addition, processing data collected for one purpose for another incompatible purpose (where an exemption does not apply) is a breach of UK GDPR. The framework's governing body should therefore have a significant role in ensuring data used in digital identity is limited for this purpose in practice.

Automated processing

Concerns and potential risks may arise for individuals if digital identity and attribute systems (or the service providers consuming digital identity and attributes) rely on automated processing. This could include use of algorithms or artificial intelligence as part of the system. Article 22 of the UK GDPR restricts solely automated decision-making that has a legal or similarly significant effect on an individual. person. As well as there being a requirement on controllers to carry out a DPIA, solely automated decision-making that has this effect should not be carried out:

- without the informed and specific consent of the individual;
- unless it is necessary for a contract between the data subject and controller; or
- unless the law authorises it with safeguards.

Even automated processing not covered by Article 22, for example where the processing is not solely automated or it does not result in a legal or similarly significant effect, organisations still need to fully consider and comply with data protection rights and obligations. In particular, transparency, accuracy and redress mechanisms become especially important when organisations process data automatically. Therefore, we recommend that Government and organisations operating within the framework should give particular attention to this point.

Carrying out automated decision making can raise ethical considerations and relates to the UK GDPR's fairness principle.[9] Government need to fully consider this as part of the project's development. Many of the use cases for digital identity and attribute systems to aid the assessment of eligibility will be straightforward and should not raise concerns, but the risks of each use case. Government should give particular attention to the impact and risks of using special category data as an attribute. An individual may have little choice in certain scenarios and the outcome could have a significant effect on them. An assessment would need to address the necessity and proportionality of using this data, alongside any risks of an unfair outcome from using automated decision making.

Automated decision making has the potential to cause discriminatory effects. Bias in system design, algorithms or datasets can lead to outputs that affect particular groups. Some effects are expected or even desirable, such as age verification systems that restrict access to under-18s for particular services. Other bias in automated verification systems is either undesirable or discriminatory, or both.

Systems that provide eligibility as well as identity checks have the potential to result in greater harms, so particular care is needed around how such decisions are taken and whether automated decision making occurs. Our guidance on AI and data protection outlines some of these effects and how they can be mitigated. All automated verification systems need regular monitoring and mitigations need to be in place to prevent discrimination. As part of this, we welcome the trust framework's recognition of the potential discriminatory biases in automated decision making and for an appropriate governing body to receive annual exclusion reports.

Children

Children have a greater likelihood of denial of service, which may be intentional, ie through age verification schemes to prevent the purchase of alcohol. However, denial of service could be an unintended consequence of an inappropriately designed system, whereby children are eligible but denied access. This could be as they are unable to prove their

[9] The ICO recently held a public consultation on the role of data ethics in complying with the GDPR. We will be producing a response to this in due time.

eligibility, due to insufficient attributes being available to verify their identity. For example, if applying for a free or discounted travel card young people have to prove they are eligible, but may not be able to do so if they do not have the sufficient attributes to do so, such as a passport.

The UK GDPR notes that children generally merit specific protection due to the risks posed from collecting and processing their data. Therefore, any digital identity system needs to give special consideration to how it safely accommodates and protects children. Undertaking a data protection by design and default approach, and where relevant conforming to the ICO's Age Appropriate Design Code, helps to mitigate such risks.

Lawful, fair and transparent processing

One of the core principles of data protection legislation is that organisations need to process personal data lawfully, fairly and in a transparent manner.[10] Therefore, in order to be compliant with data protection legislation, each certified organisation that is part of running a scheme must:

- have a lawful basis for processing personal data;
- be fair; and
- provide clear, accurate information to individuals whose data they process within the digital identity system.

A lawful basis under Article 6 of the UK GDPR must be identified for any processing that takes place. Consideration should be given to which lawful basis is most appropriate in each circumstance. If special category data[11] (such as the provision of attributes relating to ethnicity data or provision of eligibility checks using health data) or data relating to criminal offences will also be processed by a scheme, additional requirements must be met.

We welcome the importance placed upon individuals having control over their data in the framework. It is important that individuals are offered genuine choice over whether any digital identity and attribute scheme processes their data. However, organisations need to be particularly careful seeking consent or explicit consent as a condition of accessing a digital identity and attribute scheme in the framework. Consent is likely to be invalid if they are in a position of power over the individual, for example a public authority or potential employer asking for confirmation of a medical screening. It is therefore important that consideration be

[10] Article 5(1)(a) of the UK General Data Protection Regulation

[11] Special category data is defined in A9(1) of the UK GDPR.

given to whether (explicit) consent is the most appropriate lawful basis (and condition for processing special category data) for organisations to rely upon within the design and operation of the trust framework.

The fairness principle means only processing personal data in ways that people would reasonably expect and not in ways that have unjustified, adverse effects on individuals. Therefore, all organisations within the trust framework need to consider not just **how** they can use digital identities and attributes, but whether they **should** in any given scenario. Assessing whether the processing is fair can depend on how they obtain the personal data. This is particularly relevant in relation to digital identities and attributes and links to the considerations we outline in the purpose limitation section below. If organisations deceive or mislead anyone when they obtain the personal data, then this is unlikely to be fair.

Effective transparency can unlock trust and confidence in the system. For processing to be transparent, organisations must be clear, open and honest with people from the start about who will use their personal data, how it will be used and for what purpose. In communicating about digital identities and attributes to the public, it is important that this information is user-friendly and easily understood by people who are not technical specialists.

There should also be an appropriate degree of consistency between different controllers and the privacy information they provide. The design of this new system should also create an opportunity to draw on best practice in terms of transparency built into the service experience, not just formal privacy notices. This should also include user experience (UX) testing and design. Articles 13 and 14 of the UK GDPR set out the transparency requirements and we produced guidance on the right to be informed which sets out further detail available here.

Data minimisation

Data minimisation is a core requirement of data protection legislation. When people are asked to provide more personal information than is necessary it increases the data protection risks and can diminish public trust. For example, if organisations collect excessive data for identification, there could be “function creep” and the data is seen as valuable for marketing. There are also risks if multiple organisations hold duplicated data that could be hacked or misused. Organisations must therefore ensure that personal data is adequate, relevant and limited to what is necessary for the purposes for which it is processed. They should only process data necessary to verify an individual's identity or their attributes.

Acquiring, using and retaining the minimum amount of data necessary reduces privacy risks, so any scheme within the framework should support this. In particular, organisations need to address and mitigate any unnecessary personal data trails being left when individuals use digital identities on different services. Additionally, organisations should only have access to the data that they need to carry out their services, such as receiving the verification of facts rather than the transmission of detailed information. The proposed model would support this approach but should be consistently applied throughout the system.

Storage limitation

Organisations should not keep data for longer than is necessary for the purposes for which they are processing it. This links to the requirements above for data held in schemes across the framework to be accurate and kept to a minimum. This reduces privacy risks and the likelihood that data is inaccurate or out of date, such as having a person's old address or contact details.

To comply with the UK GDPR's documentation requirements, organisations need to establish and document standard retention periods for different categories of information they hold. It is also advisable to regularly review these retention periods and ensure there is flexibility to delete data earlier than the retention period if organisations do not use it. This is particularly important where they hold special category data.

Security

Organisations operating in the trust framework must have appropriate technical and organisational security measures in place to protect the personal data held in the system. This security must be appropriate to the risk and should take account of "the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons".[12]

In practice, this means any scheme should be based on strong technical and organisational security arrangements. This is due to the attractiveness of the data in digital identity systems to bad actors, and

[12] Article 32(1) of the UK GDPR

the high risk it poses if they compromise the data. Such measures might include the use of privacy-enhancing technologies to minimise the risk of fraud, impersonation and other misuse or loss of data. Organisations should keep security measures under regular review to ensure their effectiveness, including the monitoring of false positive rates. The distributed, decentralised model can also support the effectiveness of these measures, alongside joined-up threat assessment and intelligence about risks.

A successful digital identity system will be a key component of our national digital infrastructure, part of the daily lives of the UK public and may often involve data that the public are legally obliged to provide to different government services. The focus on security will need to be match this level of importance and therefore the risks of attack. Effective safeguards will be vital in ensuring trust and confidence. The UK has a strong record in supporting effective cyber security practice, including the work of the National Cyber Security Centre, and the ICO is positive that this can be leveraged to provide strong safeguards.

Recommendations relating to interoperability and eIDAS Regulations

Trust services are an important building block of a modern global economy, providing third party assurance, security and trust between relying parties. Therefore, any digital identity infrastructure needs to support trust services in building secure cross-border services. In order to effectively do this, alignment or interoperation would be highly beneficial to ensure common assurance for organisations making use of trust services or involved in digital identity systems both domestically and internationally.

The UK eIDAS Regulations (eIDAS) set out rules for UK trust services and establishes a legal framework for the provision and effect of:

- electronic signatures;
- electronic seals;
- electronic time stamps;
- electronic documents;
- electronic registered delivery services; and
- certificate services for website authentication.

EIDAS is regulated by the ICO. There are a number of areas that require further consideration in relation to the proposed framework and eIDAS.

We will continue to engage with Government on these areas as proposals are developed.

Setting UK technical standards for trust services

Following the UK's departure from the EU, the Government may want to move away from eIDAS and set specific UK technical standards for trust services. We understand the desirability of this, however it is important that any change is carefully managed in close dialogue with relevant stakeholders (including the ICO, UKAS, Trust Services, Conformity Assessment Bodies, and relying parties). This is to avoid unintended consequences, ensure maintenance of high standards and facilitate interoperability beyond the UK.

Further clarity is needed on the role any new UK-specific technical standards/certification schemes (which do not currently exist) will play in ICO qualified trust service provider assessments and whether use of ICO-qualified trust services will be required when trust services are operating within the framework. The ICO acknowledges that this has wider applicability than to this proposed framework, and we will be pressing Government for clarity on this. In addition, it is important that sufficient notice of any divergence from existing technical standards is given. This is to ensure that existing certification schemes can be adapted to meet new requirements and new schemes can be created in good time. Finally, clarity should be provided on which body would be responsible for designing, developing and monitoring technical standards.

Mutual recognition

In addition to the above, the ICO understands the desirability for the UK to have the ability to decide on its own recognition of equivalent international trust services. Such a process would need to be clear and defined, with an appropriate designated body with responsibility for managing that recognition process.

Role of trust services in a digital identity and attribute framework

There are questions around the specific role that trust services, and our supervision of them, plays in the digital identity framework. In particular, Government should consider the following:

- What role would electronic signatures or seals play in the creation of verified attribute providers?

- What technical standards, certification schemes and level of assurance is needed for trust services operating in the Digital ID framework – in particular will qualified trust service provider status will be a necessary condition for trust services operating in the framework?

- What types of digital identity would they permit for identity verification when requesting certificates for the creation of electronic signatures or seals?

- How would the framework use trust services?

Conclusion

The ICO supports the introduction of a UK digital identity and attribute framework. Such an overarching framework can bring many economic as well as privacy benefits over reliance on paper identity records. Government's proposed framework and accompanying governance regime also has the potential to bring individual protections and trust to the existing digital identity ecosystem. However, development of the framework must proceed carefully and in accordance with data protection law.

There will be a good opportunity to embed accountability from the outset. Schemes within the framework should recognise the importance of meeting the requirements of the UK GDPR accountability principle as part of participating organisations' compliance with data protection legislation. We welcome Government's ongoing commitment to a data protection by design and default approach and hope the positions set out above are helpful in that regard. We will keep these positions under review, taking into account developments in the digital identity and attribute landscape and the feedback to the DCMS trust framework survey.

We look forward to Government's continued engagement with us on this project and are keen to provide input in an advisory and regulatory capacity as it develops. We also look forward to consultation on future legislation and DPIAs where useful or as required by law.

The formal obligation to undertake a DPIA may not apply to Government in their policy making capacity when they are not a controller but given the scale and scope of the trusted digital identity system, we highlight the benefits of an overarching assessment of privacy risks linked to the framework. This could address many of the same questions as a DPIA and can look at the risks more broadly across the proposed ecosystem. Their assessment may in turn help individual controllers assess compliance, their own DPIAs and risk of harm to individuals prior to implementation.

Annex - International models of digital identity verification

Digital identity verification has and is being implemented internationally through a variety of schemes and frameworks. These are at varying stages of development and have differing levels of data protection underpinning them. It is important for Government to keep abreast of international developments to ensure any digital identity infrastructure adopted benefits from the findings and learnings of other countries' initiatives.

The United Nations' Sustainable Development Goal 16.9 aims to provide legal identity for every individual globally by 2030 and we acknowledge that digital identity solutions have a key role to play within this. The World Bank is driving global efforts to build inclusive and trusted digital identity frameworks through its Identification for Development (ID4D) initiative, such as by publishing a guide to digital identity and data protection. We recommend the UK Government work with other countries and organisations to assess best practice internationally in order to meet this goal.

For example, Australian, New Zealand and Canadian digital identity models are all based on a trust framework, taking a similar federated approach to the approach the ICO understands Government is taking.[13] For example, the Canadian province of British Columbia used an electronic identity as its standard approach to authenticating citizens' identities for over a decade.[14] A core feature of these models is that they are optional and users can still choose paper-based, phone or in person options instead, which we recommend the UK's digital identity ecosystem replicates.

Sweden, Norway, Finland and Denmark also all have widely adopted digital identity systems that are used by over 70% of their populations.[15] A key element of their success was government working with industry, such as organisations in the banking sector. We support engagement with sectors, organisations and researchers that will operate a digital identity

[13] For Australia see https://www.dta.gov.au/our-projects/digital-identity, for New Zealand see https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/about-the-digital-identity-programme/ and for Canada see https://diacc.ca/

[14] https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/identity-and-authentication-services/bceid-authentication-service

[15] https://www.computerweekly.com/opinion/What-the-UK-can-learn-from-the-Nordics-when-it-comes-to-digital-ID

system to ensure it is fit for purpose and data protection by design and default is baked into the system.

Interoperability with other international digital identity solutions is also important to enable UK citizens to use their digital identities in other countries and for citizens of other countries to use their digital identities in the UK. We recommend that any international interoperability should maintain an equivalent level of personal data protection as the UK model provides.

Whilst it is important to collaborate with other countries, consideration should be given to the importance of upholding citizens' privacy and their ability to choose whether to use a digital identity or a paper-based alternative. Whilst Estonia has one of the highest rates of citizens using digital identities to access services at over 98%[16], we note that Estonia has a mandatory requirement for citizens to hold a national identity card, which contributes to the uptake of a digital identity. We understand that in the UK, digital identities will be entirely optional, as the UK does not have national identity cards nor any plans to introduce them.

In particular, consideration should be given to the scope of any international digital identity solutions and how the data enabling the digital identity will be used. Creating prescribed use cases will be beneficial in ensuring that UK digital identity solutions are only used in appropriate circumstances.

[16] Figure correct as at 15 March 2021 in relation to those using the Estonian ID card that can be used in electronic environments for services such as electronic prescriptions, logging into bank account and for digital signatures. Source: https://e-estonia.com/solutions/e-identity/id-card