BIG INNOVATION CENTRE

National Data Strategy Consultation Response

Advisory Board Members of the APPG AI and APPG Blockchain Working Groups.

November 2020

Background

Earlier in September, the Department for Digital Media and Sport published a call for an open consultation which offers stakeholders the opportunity to advise on the UK National Data Strategy proposal released on the 9th September 2020.

The Advisory Board Members of the All-Party Parliamentary Group on Artificial Intelligence (APPG AI) and All-Party Parliamentary Group on Blockchain (APPG Blockchain) have joined forces to submit a response to this government consultation.

Focusing on the core principles of the National Data Strategy, the consultation is built around five main pillars or missions, with concrete questions for each area. In order to respond to this consultation, five working groups were set up, one for each mission:

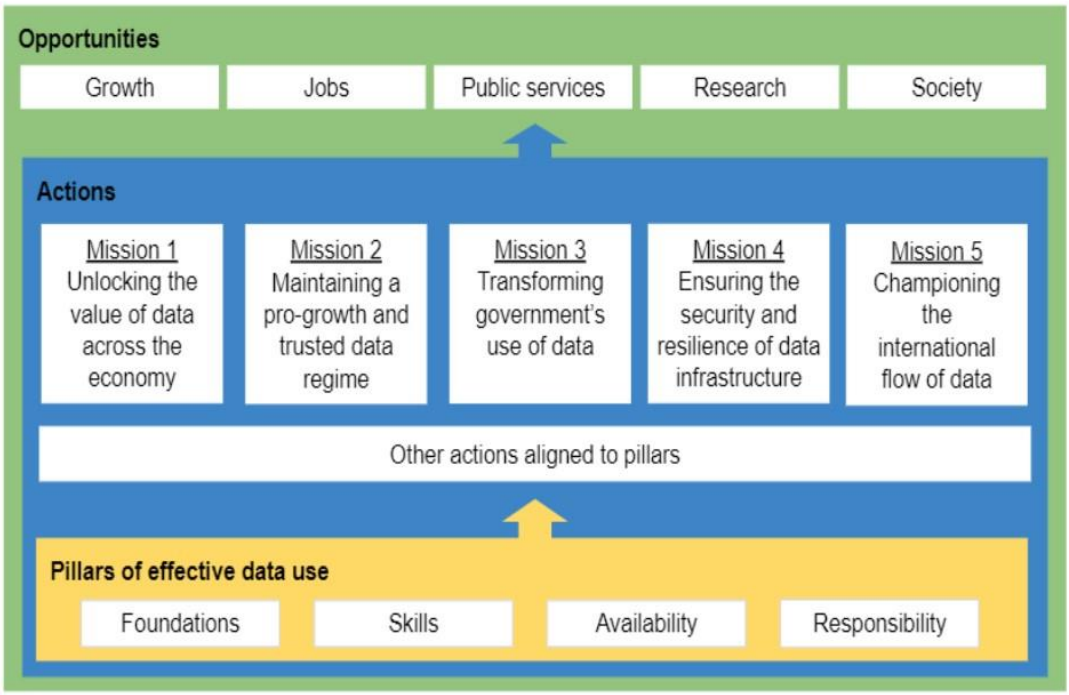

Figure 1. Pillars, missions, and opportunities of the National Data Strategy

The Working Group

The submitted consultation paper is the result of a joint project of expert advisers and corporate members of the advisory boards of the All-Party Parliamentary Group on Blockchain and All-Party Parliamentary Group on Artificial Intelligence.

Working Group Members

- *Charles Kerrigan*, CMS, Partner & Global Head of Fintech
- *Chris Francis*, SAP, Director of Government Relations
- *Del Alibocus*, Capita, Group Consulting Head of IoT
- *Doug Brown*, Capita, Chief Data Scientist and Head of Data and Artificial Intelligence Guild
- *Florentin Albu*, Utility Computing, Chief Digital Technology Strategist
- *James Kingston*, Hatlab, Director
- *Kenan Direk*, UCL, Research Data Manager
- *Martin Venn*, Venn Consulting, Lead Consultant
- *Matt Stagg*, Capita, Data & AI Solutioning Lead
- *Michele Nati*, IOTA Foundation, Head of Telco and Infrastructure Development
- *Oner Avara*, My Next Match, CEO
- *Professor Birgitte Andersen,* Big Innovation Centre, CEO
- *Scott Stainton*, Capita, Senior Artificial Intelligence Scientist
- *Shaun Barney*, Capita, Senior Artificial Intelligence Scientist
- *Tim McGarr*, British Standards Institution, Sector Lead (Digital)
- *Tirath Virdee*, Capita, Director of Artificial Intelligence
- *Tulsi Parida*, Visa, Senior AI & Data Policy Manager

Project Managers & Rapporteurs

- *Dr Désirée Remmert*, Big Innovation Centre, APPG on Artificial Intelligence Project Manager
- *Fernando Santiago-Cajaraville*, Big Innovation Centre, APPG on Blockchain Project Manager

The All-Party Parliamentary Groups on Artificial Intelligence (APPG AI) and Blockchain (APPG Blockchain) are hosted in the UK Parliament. The APPGs provide evidence, use cases, and future policy scenarios, and analyse the industry, economic and societal implications of AI and Blockchain technologies.

<u>This consultation paper does not represent the opinion of the APPGs, or the Parliamentary Members of the APPG AI and APPG Blockchain.</u>

1. Contents

Framing and Core Principles

Q1. Do the missions and pillars of the National Data Strategy focus on the right priorities? Which areas should be explored in further depth?

Strongly disagree

The proposal for the National Data Strategy outlines an adequate approach by defining the main thematic pillars and proposing actions to overcome the major barriers in these areas. However, we are highly concerned that the proposal fails to tackle the major problems in the areas of data governance, ownership, and management.

From our point of view, the strategy touches upon important issues of data governance but falls short in proposing solutions to important future challenges which will accompany the newest technological developments. We thus suggest a revision of the national data strategy that takes into account the challenges that new technologies - as 6G, edge-AI, connected cities or connected entities - will bring to the data governance.

This apparent lack of ambition of the National Data Strategy could result in slowing down the conversation about the priorities for data at the national level and, as a consequence, negatively affect economic development.

In order to meet the objectives laid out in the current NDS proposal on the use of data, which include for example “help organisations of every kind succeed”, “delivery of existing services, from manufacturing to logistics”, “drive of scientific and technological innovation*” or “tack climate change”* to keep the United Kingdom as leading digital nation, we consider, the final Data Strategy should:

Ensure the appropriate use of data

Currently, it could be argued that data is being unnecessarily collected, processed, and stored, regardless if it offers any real insight. For this reason, the government should take a more directed approach to ensure data use is appropriate and in line with the GDPR, making the rationale transparent for the intended audience.

Reconsider how data is collected, evaluated, and used

Being aware that the way data is collected, processed, and interpreted has real traction in terms of process issues.

The National Data Strategy must consider how data is going to be collected, evaluated, and used.

The process of collecting, evaluating, and using data from government departments should be homogeneous and straightforward regardless of the department which "owns" the data.

To achieve this, we recommend making available the analytical code behind the analyses. Using this method to render results more transparent could also increase public trust in government reports.

As an example, it should be a straightforward process from reading a government published technical report to identifying the dataset(s) used and links to other work by/or behalf of the government that uses the same data. Current Defra Data governance could be an internal example to follow.

Define a clear path to reach data transparency

Although "transparency" is named in several sections of the National Data Strategy (Missions 3 & 5, Sections 6.1, 6.3, 7.1 & 7.2) the document does not state a clear path to achieve it.

There is a need for a system or scheme where the government caters to a broad user base, both individuals and institutions, independent from government, that arguably should be granted with access to non-open data through sensitivity tiers and secure environments.

Create channels of communications

As experienced users of data published by the government, there are many opportunities to improve both the transparency and usability of data resources.

Current structures lack the necessary formal "communication channel", a place to provide feedback or suggestions on the service.

The creation of a formal channel of communication could contribute to improving the government's use of data and help shape future data systems.

Embrace practices/solutions in the public and private

Recent events (notably, contact-tracing and Windrush) have hurt the public perception of data competency within the government and does a great disservice to those working in or with the Civil Service.

The transformation of government data use cannot be done without an evaluation of the current data processing procedures. Ineffective, underutilised, and inappropriate processes should be adequately identified to improve them.

Explore the creation of data marketplaces

The amount of data being produced far exceeds the capability of humans to curate and consume it. A marketplace for data is needed at a national level, that is consumable by humans and by machines.

Utility and monetisation aspects of data should be analysed as part of the National Data Strategy. The creation of data marketplaces for the establishment of enterprises might enable the cataloguing and curation of data.

We recommend exploring appropriate decentralised models to enable data discovery and usage.

Revise the data property approach

There are certain approaches in the document where it is suggested that personal data (e.g. health data) and non-personal data (company data) belongs to the state. This approach seems questionable due to the risk to alienate those institutions, corporations, and individuals that do not agree.

Examples in the current National Data Strategy proposal
Section 2.1 -*"Data is knowledge. By having access to more of it [...] we get greater insight into what works and what does not – both in terms of selling products and services, and in terms of making our own processes and practices more efficient".*
Pilar 3 - Data availability: *For data to have the most effective impact, it needs to be appropriately accessible, mobile and re-usable. That means encouraging better coordination, access to and sharing of data of appropriate quality between organisations in public, private and third sectors.*

Include machine learning models

Machine learning models should also be tackled by the strategy along with processing capabilities and sharing of curated training data sets.

Data availability will not correspond to the ability to extract value from it if the infrastructure is not provided. It will not change the current situation where only the ones being able to do so are the ones that already have the data.

Q2. How could data have been used more efficiently to deliver public benefits during the coronavirus (COVID-19) pandemic beyond its use in health and social care?

For question two, we are only looking for examples outside health and social care data. Health and social care data will be covered in the upcoming Data Strategy for Health and Social Care.

Data generated in public transport could have been used to predict when and where the crowding of stations and trains would occur (and hence when social-distancing protocols were likely to be broken). To expect people to follow social distancing rules without setting in place specific mechanisms to facilitate rule-abiding behaviour might have been overly optimistic. TfL, for example, can determine the number of people that get on and off at stations. This applies to all other forms of transport, too. The challenges brought about by the pandemic, however, have demonstrated that existing strategies that enable contact tracking are not reliable.

Further, data from testing centres and hospitals could have been used to effectively analyse the growth of clusters in a way that does not impinge upon privacy. In this context, a self-sovereign digital health passport, which also offers insight into contacts with Covid-19 hotspots as well as digitally signed test results, could have helped reduce the more drastic measures taken to guarantee the safe use of public transport.

Moreover, we suggest focusing on the short and long-term impact which COVID-19 will have on energy demand. The pandemic is likely to have a lasting societal and economic impact. Therefore, it is important to understand the new energy demand profile and potential impacts on future carbon emissions and reduction strategies. We are not aware of any government data resources that offer sufficient granularity for this type of research. For this reason, the government should support initiatives that utilise the smart meter implementation programme through publishing data that can be linked to at a household level (e.g. English Housing Survey). If we have to wait 6-12 months for data, it hinders our ability to support the government in its time-sensitive situations (such as COVID-19) and rapidly diminishes any value it once had.

Q3. Which impact might the proposals outlined in the consultation have on individuals with a protected characteristic under the Equality Act 2010*?*

We agree that the proposals outlined are comprehensive. However, it must be guaranteed that processes are in place, which ensure that automated tools are compliant with the respective regulations.

Further, we recommend offering minority groups and individuals with protected characteristics free training that develops digital literacy. This training should consider the specific demographic background of societal groups to convey digital knowledge and skills effectively. The courses should inform about privacy rights and issues surrounding data privacy when using online services.

Q4. What impact might the proposals outlined in this consultation have on the UK across all areas? How can the government ensure that regional inequalities are taken into account?

There are substantial regional disparities across the country due to varying population density and demographics, as well as the density of data collection devices and infrastructure. In addition, there are regional differences in terms of jobs and lifestyles.

These will be reflected in data related to social services and medical records. This does not detract from the fact that there are unresolved issues around data governance in particular regional industries that need to be supported. For example, some Scottish regions might want to capitalise on the data that support their local industries. Issues around data are likely to be influenced by political objectives rather than being simply business-oriented. For this reason, it must be ensured that there is a level playing field whilst guarding regional and national interests.

Mission One: Unlocking the value of data across the economy

Data is an incredibly valuable resource for businesses and other organisations, helping them to deliver better services and operations for their users and beneficiaries. However, there is increasing evidence to suggest that the full value of data is not being realised because vital information is not getting to where it needs to be.

Our first mission is to create an environment where data is appropriately usable, accessible and available across the economy – fuelling growth in organisations large and small. We will create a clearer policy framework to identify where greater data access and availability across and with the economy can and should support growth and innovation, in what form, and what government's role should be, in the UK and globally.

Data availability: For data to have the most effective impact, it needs to be appropriately accessible, mobile and re-usable. That means encouraging better coordination, access to and sharing of data of appropriate quality between organisations in the public sector, private sector and third sector, and ensuring appropriate protections for the flow of data internationally." (UK National Data Strategy Consultation September 9)

Q5. Which sectors have the most to gain from better data availability?

- Agriculture, Forestry and Fishing
- Manufacturing
- Mining and Quarrying
- Real Estate Activities
- Water Supply and Waste Management
- Wholesale and Retail Trade

Overall, all the listed sectors on the consultations would benefit from better data availability.

When discerning sectors which will benefit most from better data availability, we must consider that any sector has enormous potential to gain from improved data availability. However, if the government would like to focus on specific sectors, the following actions should be taken into account.

Determining metrics for impact assessment

To decide whether a sector would benefit from improved data accessibility, the government should put in place the criteria to assess its impact on a given sector. The government should assess in which areas greater availability of data would improve

competition on service and value, instead of simply superiority of data possession by organisations.

In our view, areas one should focus on are those where there is a high potential signal value of data, high data mobility, and a high number of interactions between service providers and service users. Once these areas have been located, the government can take steps to improve data liquidity.

Discern between personal and non-personal data

There is a need to distinguish between the better availability of personal and non-personal data. The use of personal data might create more GDPR issues; Therefore, the group considers that it would be better to focus first on those sectors that can gain from better availability of non-personal but proprietary data.

Focus on sectors with less digitalisation

The government should take into consideration those sectors that have seen less digitisation until now. The potential to leverage the benefits of better data availability will be higher, and these sectors could represent better opportunities for leveraging overall data accessibility. Among these sectors with less digitalisation, we could consider,

- Agriculture. Although digitisation has increased in recent years, data is hardly shared outside of a single producer/farmer domain, mainly due to the lack of trust among stakeholders. However, there is a growing need for the public to understand farming practices and product provenance. This is only possible if farmers are guaranteed to retain enough control over who accesses their data. This concerns for example, the fish and salmon industries.
- Mining and quarrying. With a lot of issues in terms of the environmental impact of the activity and health and safety conditions of these businesses, better availability of data will increase the transparency of this industry, increasing public trust in it and catalysing their expansion.
- Water supply and waste management. A sector that is still behind other utility activities, for example, in the energy sector, the use of smart metering. It will provide the customer with the opportunity to make more informed choices, consequently improving competition in the sector.
- On-demand manufacturing and customisation. Although digitalisation is slowly taking place, the lack of data sharing within the sector is still the main barrier. Due to confidentiality concerns, suppliers hesitate to share data that might increase the traceability of their distribution chain. Nevertheless, better data availability means a better match between supply and demand and, consequently, a reduction in the waste and environmental impact of the sectors, a reduction in the transportation cost, and an improvement of the circular economy.

Q6.- How could the central government enable better availability of data?

The government should take steps to enable individuals to gain and realise the value in the data produced by them.

In general, the government should be doing more to enable data trusts and other collaborative and intermediary entities. We recommend some of the actions that the government should take in order to provide better data availability,

Support the infrastructure set up

The central government should support the creation of a data trust infrastructure. We suggest, however, that although the government should support this infrastructure, it should not be owned by it. The infrastructure should be developed based on the latest technologies, including distributed ledger technology.

Data integrity, accountability, and incentivisation to not host data itself should be part of the initial design requirements. Principles of open source, shared ownership, public contribution, and support should be considered.

As an example, the European Commission supports the creation of the EBSI (European Blockchain Services Initiative). It will allow the public and also private organisations to develop applications that connect to and make use of the EBSI infrastructure with common standards.

Support data portability

Data should be maintained in their original repositories, and with their original data creator, however, data portability should be encouraged. This requires a definition of standards for data interoperability and portability.

The right incentives and accountability for the contributions of each data provider should be put in place.

Put in place regulation & standards

The government should consider the impact of legislation as a potential tool to incentivise competition. Better and more regulation on data ownership, data accountability, and monitoring is needed. Standards for data transparency (i.e., data labels or personal data receipts) should be defined.

An interesting example is the “21st Century Cures Act” in the USA. The act provides

interoperability standards and the right of access to US health personal data.

Increase data awareness

The government should create and support data literacy across all of society, in particular, to foster the sharing of personal data. A focus on data rights, ownership, and enabling individuals to access and control their own data will help with this.

As an example, a new wave of tech infrastructure companies is enabling this. Solid and Dataswift provides individuals with the means to legally own and control their personal data, and to transact upon it

Other actions to consider:

- Develop testbeds to understand the benefits of data sharing.
- Provide data registration and data discovery services (eventually centralised).

Q6a.- How could this role vary across sectors and applications?

The role of government is to ensure that regulations for current laws are enforced.

The role of the government should vary depending on the area,

- From an **infrastructure perspective,** the role of the government should be cross-domain.
- From a **policy perspective,** it should depend on sector-specific regulations. However, the policy concerning consumers and their data should be homogenous to avoid confusion.
- **Transparency principles** should be done cross-domain. This requires fostering cross-sector collaboration on data transparency principles.

Data owned by the government

Currently, the full value of the data cannot be leveraged as the data exists in a form that cannot be utilised in an effective and relevant way. The sets of data made available by the government should go through standardisation processes and filters that ensure compliance and made available on a real-time basis.

Q7. Which role should the government play in supporting data foundations in the wider economy?

We partially agree that the government should support data foundations in the wider economy. We need greater government involvement in encouraging ideas, enabling them to become viable, and delivering values and economies. In order to do this, we recommend the following actions:

Set up standards on interoperability

The government could **set standards on interoperability** with regards to data types, formats, and APIs to be used. Legislation can be used to force organisations to release data deemed of use to the broader public or economy, enabling more innovation.

Lead the strategy

The government is responsible for designing strategies and articulating a better breed of policies for private enterprises.

It is in the national interest to enable private enterprises to learn from each other in an open way. Whilst it is not the place of the government to create a national enterprise-related data, it can encourage the sector to support the data economy as an essential part of the future of the economy.

Support infrastructure

The government could explore different models of a cooperative data infrastructure. An infrastructure to support the data foundations on a broader economy is needed.

Although the government can facilitate this data infrastructure, some sensitive aspects deserve attention. Holding data could lead to fear of being controlled, spied on, especially when it is about public and consumer data. Infrastructure should be shared and open. Best practices should be mandated and audited but not enforced in a controlled infrastructure.

Q8. What could central government do beyond existing schemes to tackle the particular barriers that small and medium-sized enterprises (SMEs) face in using data effectively?

Smart Data Review should empower the Individuals

According to the Smart Data Review, *"The focus is citizens asking their providers to share information about them with third parties"*. However, we recommend putting the focus on "Providers providing the data that the individuals generate, to the individuals themselves".

Individuals should be allowed to own, control, and transact with their own data.

Individuals are far better placed to choose what is right and appropriate for them than organisations. The government should empower individuals with a place to store data and with the ability to transact data. Highly mobile data will lead to 'smarter' data and increase the overall data exchange.

SME use of data

Facilitate access to data scientists. SMEs face a shortage of data scientist skills and data processing infrastructure. These are usually captured by large corporations together with a more considerable amount of data, particularly useful for artificial intelligence and machine learning.

The creation of accelerator programs for SMEs to access data within frameworks that define the right incentive for companies to open up their data, guarantee data ownership and revenue sharing.

Data processing infrastructure

The government should facilitate the creation of a data processing infrastructure that incentivises the share and access to data. Internationally, we have seen the creation of data marketplaces in other economic areas around the globe.

Q9. Beyond existing Smart Data plans, what further work should be done to ensure that consumers' data is put to work for them?

Actions to consider:

- Define a set of open APIs like in the banking system. Facilitate the creation of task forces for their definition.
- Define the principles for transparency on data sharing and adopt them across industries.
- Empower consumers with the ability to share their data easily
- Control the transparency of the use of data from 3rd parties
- Provide the consumers with the ability to retract data access
- Encourage the exploration of tools such as labels and personal data receipts

Besides the government should,

- Explore data exchange platforms
- Explore business data objects
- Ensure technologies such as lakehouses and valuation mechanisms exist.

Mission Two: Maintaining a pro-growth and trusted data regime

"Building on our status as a world leader in technological innovation and our robust data protection standards, we will maintain a data regime that supports the future objectives of the UK outside of the EU and promotes growth and innovation while maintaining public trust. This regime will not be overly burdensome for the average company, nor will it be unnecessarily complex or vague; it will help innovators and entrepreneurs use data legitimately to build and expand their businesses, without undue regulatory uncertainty or risk at both the domestic and international levels.

To encourage the widespread uptake of digital technologies, we will also work with regulators to provide advice and support to small- and medium-sized businesses to help them expand online, and develop sector specific guidance and co-regulatory tools to accelerate digitisation across the UK economy." (UK National Data Strategy Consultation September 9)

Q10. How can the UK's data protection framework remain fit for purpose in an increasingly digital and data-driven age?

Remain Aligned with the General Data Protection Regulation (GDPR)

The Current General Data Protection Regulation, GDPR, delivers substantial benefits and is viewed positively in developing an accepted 'gold standard' of data protection that is now used around the world.

In the future, UK firms will need to comply with the GDPR and equivalent frameworks, meaning that significant divergences from the GDPR would be an additional regulatory burden for the UK firms and would cause significant disruptions in the growth of the technology sector and cross-border data flows.

Domestic Data protection framework, should remain aligned with the GDPR

Although the future domestic data framework should remain aligned with GDPR, it should, at the same time, capture the emergence and complexity of evolving artificial intelligence systems. In order to do that government should take some initiative in the following areas,

Portability of personal data

A personal data protection framework should embed principles such as interoperability, data portability and user control, encouraging companies to support such principles.

Most of the personal data is generated directly by end-users. Data protection should include not only the principle of controlling access (meaning privacy) but also securing access.

Proprietary data accessibility

There is currently a lot of untapped value in proprietary data which is even less accessible to small and medium enterprises than personal data. The abundance of such data cannot be generated by a single successful mobile app.

Sharing of such data is mainly limited by the risk of confidentiality breaches as well as by IPR issues that might arise when new AI models are developed. Such aspects should be considered and further included in any data protection framework.

Guidance support

To aid organisations with data protection, focusing on existing guidance (e.g. ISO/IEC), rather than developing further UK specific guidance and additional activities for UK firms or firms looking to work in the UK

Q11. Should the functions for the Centre for Data Ethics and Innovation (CDEI) be Artificial Intelligence (AI) monitoring, partnership working and piloting and testing potential interventions in the tech landscape?

We partially agree that the above outlined functions should be within the scope of the CDEI.

The CDEI was initially set up to independently advise the government on artificial intelligence (AI) areas. For example, the CDEI has recently published some excellent papers on AI bias and online targeting.

We encourage the CDEI to continue to produce thought leadership pieces and act in an advisory capacity to the government.

There is a need for the CDEI function, which should not be lost if the scope of the CDEI changes.

We caution against duplication of efforts with other regulatory and relevant bodies in the industry.

In case the government would be willing to enlarge the scope to the CDEI, we would recommend to

- Set up a cross-domain framework.
- Increase work on definition and adoption of standardised transparency practices. Requiring transparency is too vague due to the diversity of end-users.
- Support and facilitate proper data literacy.

Q11a. How would a change to statutory status support the CDEI to deliver its remit?

The CDEI should remain independent but be funded by the government and receive input from a variety of sectors and government to the direction of the work

---

If the scope is enlarged, the current cross border approach should be carried out by the CDEI; however, it could work with specific sector bodies too, for example,

- Collaborate with the Catapults network and standard bodies (BSI)
- Create testbeds.
- Oversee infrastructure development.

Mission Three: Transforming government's use of data to drive efficiency and improve public services

"There is massive untapped potential in the way the government uses data. We will implement major and radical changes in the way that the government uses data to drive innovation and productivity across the UK. In doing so, we will improve the delivery of public services, as well as our ability to measure the impact of policies and programmes, and to ensure resources are used effectively.

To succeed, we need a whole-government approach led by a Government Chief Data Officer from the centre in strong partnership with organisations. We need to transform the way data is collected, managed, used, and shared across government, including with the wider public sector, and create joined-up and interoperable data infrastructure. We need the right skills and leadership to understand and unlock the potential of data – and we need to do so in a way that both incentivises organisations to do the right thing, as well as build in the right controls to drive standardisation, consistency and appropriate data use." (UK National Data Strategy Consultation September 9)

Q12. We have identified five broad areas of work as part of our mission for enabling better use of data across government:

While we appreciate that the government acknowledges the urgency for designing a national strategy that would allow for more efficient use of data, improved delivery of public services, and more reliable measuring of the impact of policies and programmes, we are concerned about the document's lack of clarity concerning its desired outcomes. We recommend identifying specific problems within the public sector areas (LG, NHS, Education, etc.) and designing a strategy on how the efficient use of data could contribute to the solution.

We further suggest the introduction of a separate principal unit that will regulate the use of data within the public and private sectors.

Another issue we would like to address in the context of the government's use of data is the current lack of access to data for researchers and developers. Whereas data is generated, aggregated, and stored in most public entities, a coherent method to access these resources is missing. Despite there being a number of open innovation schemes that enable the sharing of data, there appears to be a lack of motivation to participate in these schemes in the public and private sector. We, therefore, recommend designing strategies to make the sharing of data more attractive, possibly by introducing the monetisation of data, i.e. a data currency, as a significant step forward.

One way to address the above would be to create a *Government Data Exchange Service*, focused on two key groups of users, data providers and users:

Data provider's interface

- Describe the data
- Set of access controls (2FA, or decentralisation)
- File-based or API

Data acquirer's interface

- Search the market or set alerts
- Required pricing model or as is

Below is a quick representation of how such a data exchange service would enable the main functions of *governance* and *discovery*.

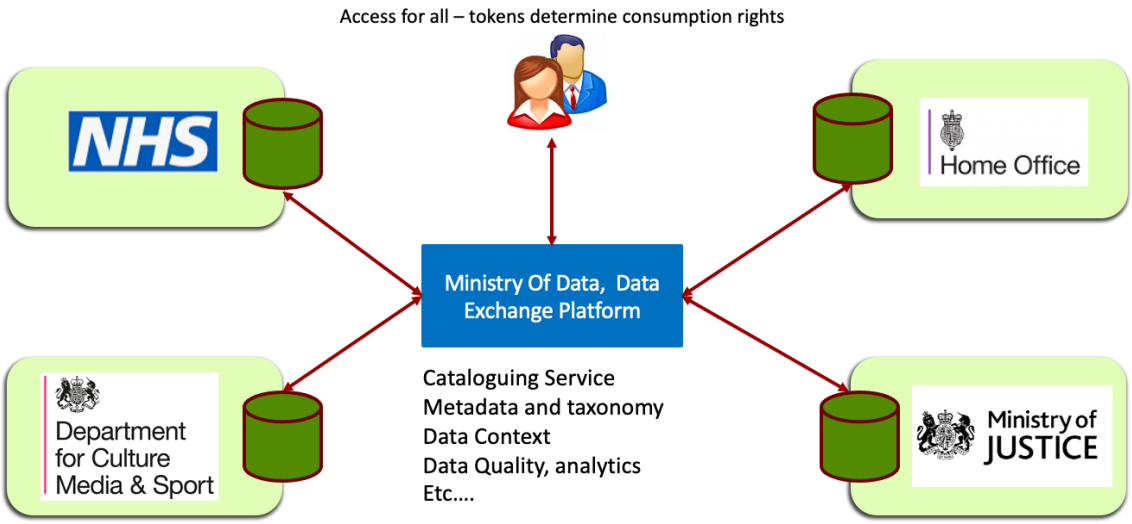

Figure 2. Role of the Ministry of Data Exchange

Several essential elements need to be incorporated into the model described above:

Data cataloguing service

- Data context
- Access tokens
- Data quality and analytics
- Glossary of data

More elements can be introduced over time, including the use of Blockchain infrastructure.

Once the above structure is in place, the government can include third-party data sets as required and with controlled access.

Q13. The Data Standards Authority is working with a range of public sector and external organisations to create a pipeline of data standards and standard practices that should be adopted.

The authors of this contribution agree that the UK does not lack data standards but lags with regard to their adoption and adequate documentation. We recommend that the Data Standards Authority (DSA) should streamline its practices and focus on providing adequate information on the standards being used for datasets. Further, we encourage broadening the scope of the community of practice group as outlined by the DSA beyond experts working within a government organisation. We fear that the current definition creates an unwelcoming atmosphere for external individuals to engage with the work of the DSA.

Moreover, whilst there certainly is not a one-size-fits-all approach, designing a consistent data cataloguing standard would facilitate the collaboration and sharing of data between departments, agencies, and public bodies.

Mission Four: Ensuring the security and resilience of the infrastructure on which data relies.

"In the UK, the government already imposes safeguards and enforcement regimes to ensure that our data is handled responsibly. But we will also take a greater responsibility for ensuring that data is sufficiently protected when in transit, or when stored in external data centres.

The government will determine the scale and nature of risks and the appropriate response, accounting for emerging trends in the market landscape. We will also determine whether current arrangements for managing data security risks are sufficient to protect the UK from threats that counter our missions for data to be a force for good. And we will consider the sustainability of data use, exploring inefficiencies in stored and processed data, and other carbon-inefficient processes.

The infrastructure on which data relies is the virtual or physical data infrastructure, systems and services that store, process and transfer data. This includes data centres (that provide the physical space to store data), peering and transit infrastructure (that enable the exchange of data), and cloud computing that provides virtualised computing resources (for example servers, software, databases, data analytics) that are accessed remotely." (UK National Data Strategy Consultation September 9)

Q14. What responsibilities and requirements should be placed on virtual or physical data infrastructure service providers to provide data security, continuity, and resilience of service supply?

We suggest that the responsibility to provide data security, continuity, resilience, and service supply must be negotiated between the customer and the supplier. Customers should be educated on best practice principles. Further, contractual terms such as data security, continuity, and resilience must be clearly defined. However, how and to what degree these terms will be fulfilled would be dependent on the specific agreement between customers and suppliers.

We recommend considering a legal obligation on providers to be able to run a recovery playbook on a customers' demand.

Q14a. How do clients assess the robustness of security protocols when choosing data infrastructure services? How do they ensure that providers are keeping up with those protocols during their contract?

A specification of the robustness of security protocols and a guarantee that providers are abiding by those protocols during their contract should be part of the Service Level Agreements.

We recommend an orientation on the standards around common cloud SLAs as outlined in the ISO/IEC 19086-1:2016.

Q15. Demand for external data storage and processing services is growing. In order to maintain high standards of security and resilience for the infrastructure on which data use relies, what should be the respective roles of government and data service providers, their supply chain, and their clients?

Globally applied best practice guidelines on the standards of security and resilience for such infrastructures are outlined in ISO/IEC 27017 or ISO/IEC 27018. The government should help to shape these and promote them, given that this is a global market.

Q16. What are the most important risk factors in managing the security and resilience of the infrastructure on which data use relies?

A definition of the most important risk factors in managing the security and resilience of the infrastructure on which data use relies should, at a corporate level, be related to the specific organisation's risk profile. Nationally, these risk factors should be assessed by the National Cyber Security Centre (NCSC).

Q17. Should the government play a greater role in ensuring that data use does not negatively contribute to carbon usage?

We think that it should be the government's goal to ensure lower carbon usage in general. However, we would discourage government regulating how it is used within a specific business. Data processing can be power-hungry; however, singling it out might be counter-productive to the purpose of this consultation.

Mission Five: Championing the international flow of data

"In our hyper-connected world, the ability to exchange data securely across borders is essential. As the UK leaves the EU, we have the opportunity to develop a new UK capability that delivers new and innovative mechanisms for international data transfers.

Using our reputation as a world leader in digital, a champion of free trade and the rules-based international system, and an engaged, rule-abiding member of the global community, we will build trust in data's use, creating the regimes, approaches and tools to ensure personal data is appropriately safeguarded as it moves across borders. We will also facilitate cross-border data flows by removing unnecessary barriers to international data transfers that promote growth and innovation. And we will seek to promote data standards, data interoperability, and UK values internationally." (UK National Data Strategy Consultation September 9)

Q18. How can the UK improve on current international transfer mechanisms, while ensuring that the personal data of UK citizens is appropriately safeguarded?

We recommend that the UK should implement short-term alternative safeguards (e.g., SCCs, Binding Corporate Rules) until proper international transfer mechanisms are established in the post-Brexit era. In individual cases, the UK may rely on the narrow derogations set out in Article 49. For data flows outside the EU/EEA, a conflict resolution governance framework and the monitoring of third countries concerned should be integrated into corporate compliance programs.

The introduction of cross border transfer mechanisms should be transparent and non-discriminatory for local and foreign entities and provide clarity to enable compliance. In addition, the harmonising of domestic privacy and cybersecurity frameworks with regional or international standards can increase compliance. At the same time, this would reduce costs. We recommend orienting on the APEC CBPR rules regarding data protection. We further recommend orienting on the ISO 27701 and the US National Institute of Standards and Technology (NIST) framework49 for cybersecurity, which enable companies to transfer data without restrictions. If appropriate protections are in place, companies will remain accountable.

Further, consideration could be given to the establishment of data processing zones or staging areas, which could govern the transfer mechanisms. The government should also explore the option of providing assistance to developing countries to increase their standards of data transfer and to ensure compliance and frictionless data transfer within a common framework.

Moreover, the data flow between the UK and other countries, incl. EEA, with which the UK has an agreement, needs to be frictionless both ways. At present, the strategy sets out an asymmetric frictionless flow of data, with incoming data to the UK flowing freely, but outgoing data having to go through adequacy assessments. This approach might work in the case of an agreement between countries; however, this does not seem to be the scenario outlined in the National Data Strategy. Specific to EEA, as both the UK and EU have been subject to the GDPR, a frictionless symmetric flow of data could be achieved from day one

Q19. Which countries should be prioritised in future UK data adequacy arrangements, and how can the UK work with stakeholders to ensure the best possible outcome for the UK?

With the advent of Brexit and the recent European Court of Justice (ECJ) judgements indicating that individual UK legalisation convenes the current data adequacy arrangements, e.g. Investigatory Powers Act 2016, there might emerge future ECJ challenges. However, in our opinion, the main problem relates to the flow of information from the UK to other countries rather than from the UK to the EU. Therefore, we suggest adopting a post-Brexit period of grace whereby data flows can continue under the EU arrangements until a suitable adequacy framework can be agreed upon (such as the 1980 Council of Europe convention on the processing of personal data).

We suggest further segmenting the types of data that are subject to arrangements with Non-EU countries beyond personal data transfers for commercial purposes and law enforcement. The transfer could be arranged on a permission-based data exchange or passporting system. The Data Exchange could further allow for the regulatory permission of different types of data and its usage. Transactions could be recorded via Blockchain.

Similarly, the adoption of approved codes of conduct and accredited third-party certifications could provide companies with the possibility to introduce customised solutions for international transfers. These could be expressed in terms of a quality standard, e.g. a privacy seal or mark.

The use of pre-pack arrangements and toolkits such as those in the GDPR (Standard Contractual Clauses (SCCs) and Binding corporate rules (BCRs) could also be utilised. The adoption of a genesis code, e.g. origination and ownership of data as applied to non-EU countries, has merit. In the short term, compliance with the current EU standards as a minimum would facilitate trade and minimise disruption even with the absence of a governing body, e.g. ECJ. In the medium term, the UK should consider the establishment of a Data Exchange to manage the standards for international data exchange. Moreover, the UK should continue working with actors such as the United Nations Special Rapporteur on the Right to Privacy, and further develop its working relationships with

regional organisations such as the Asia-Pacific Economic Cooperation to create a multilateral framework.

Overall, considering that the details of future bilateral agreements and other operational arrangements are not known and would be hard to anticipate, we suggest that a national data strategy should be supported by a set of principles. These principles would indicate the overall aim of the strategy and should provide guidance at a future point when a specific policy with another country is defined. Such principles could define the UK's stance regarding information exchange (e.g. aiming for frictionless data flows) and clarify aspects such as commitment toward ethical use of data and towards data protection.

Contact details

APPG Blockchain Secretariat - appg-blockchain@biginnovationcentre.com

APPG Artificial Intelligence Secretariat - appg@biginnovationcentre.com

Big Innovation Centre
62 Wilson Street
London EC2A 2BU
United Kingdom

info@biginnovationcentre.com
www.biginnovationcentre.com