DCMS: UK National Data Strategy

Barclays Response

Barclays is a transatlantic consumer and wholesale bank with global reach, offering products and services across personal, corporate and investment banking, credit cards and wealth management, with a strong presence in our two home markets of the UK and the US. With over 325 years of history and expertise in banking, Barclays operates in over 40 countries and employs approximately 85,000 people. Barclays moves, lends, invests and protects money for customers and clients worldwide.

This paper provides Barclays' perspective on some of the key issues raised in DCMS's National Data Strategy consultation. We would welcome the opportunity to discuss these issues in more detail.

Data Sharing / Smart Data Frameworks

The UK's Open Banking framework has provided clear evidence of the potential benefit user controlled, real-time data sharing initiatives can deliver for consumers and the economy more broadly. However, whilst GDPR provides consumers with the right to access their data, the current lack of effective mechanisms to share that data in real time (beyond the Open Banking framework) is proving a barrier to the development of a truly Open Data economy in the UK.

Barclays therefore strongly welcomes and supports the Government's intention to extend the data-sharing principles of the Open Banking framework to other sectors of the economy through its proposed 'Smart Data' Initiatives. The Government announced its next steps regarding these Smart Data Initiatives alongside the publication of its National Data Strategy. It set out that Government would:

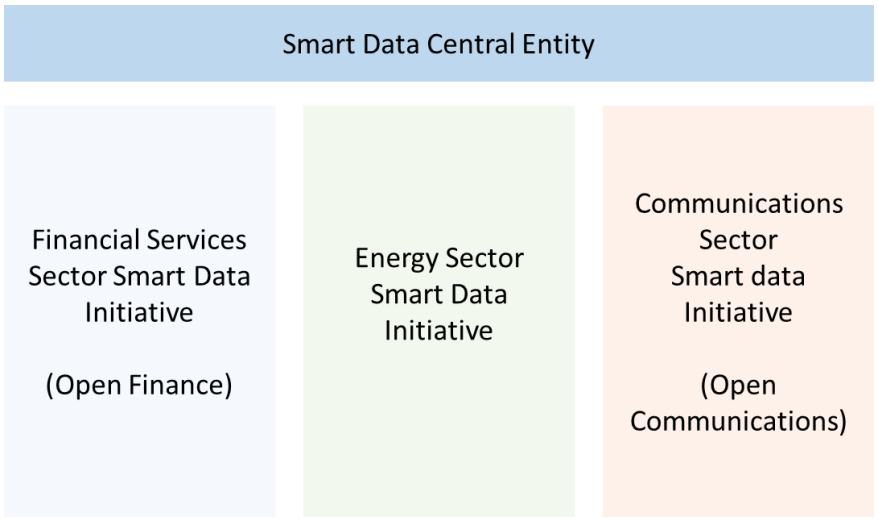
- introduce legislation, when Parliamentary time allows, extending the Government's powers to mandate participation by firms in Smart Data initiatives.
- launch a cross-sector Smart Data Working Group to coordinate and accelerate existing initiatives across regulators and government, focusing initially on communications, energy and finance. The group's remit would be to develop practical recommendations for how Smart Data initiatives could be taken forward at pace, and made consistent where feasible to avoid duplication.

<u>A Single Cohesive Framework of Sector Specific Initiatives</u>

While Barclays support the Government's intentions, we believe that it should be more ambitious in what it is setting out to achieve. Barclays would recommend that the role of the Smart Data Working Group is enhanced to create a formal, central entity responsible for bringing together the various, independent, sectoral initiatives into a single, cohesive framework for Smart Data in the UK.

This 'Smart Data Framework' could follow a two tier model, with this 'Smart Data Central Entity' being a formal, overarching authority, governing the sector initiatives below.

Proposed 'Smart Data Framework'



- Smart Data Central Entity - this central entity would be responsible for prescribing consistent operating principles and standards to be used across all initiatives, covering issues common to all such as resilience, competition, consumer protection, third party liability and a competent system of adjudication. It could also house certain shared infrastructure that could be used across each initiative, e.g. standards relating to common requirements such as consent and authentication. This Central Entity should also be responsible for promoting and incentivising participation from data holders, third parties, and customers and businesses in the various initiatives.

- Sectoral Specific Initiatives - individual sectoral initiatives would only look to develop specific APIs, standards and infrastructure where a central, cross-sectoral solution developed by the Smart Data Central Entity would be inappropriate or unworkable.

Such an approach, leveraging expertise, standards and technologies from an overarching Central Entity across all the sectoral initiatives would prove more efficient and effective than the proposed approach of attempting to coordinate independent sectoral initiatives. It is vital to avoid a situation in which different sectors implement disparate and inconsistent approaches to data sharing, as this risks limiting the development of data portability in the UK and failing to deliver the full potential Open Data has to offer.

This proposed approach to develop a Smart Data Framework would represent a significant step forward in the development of a UK Open Data ecosystem, from sectors independently implementing inconsistent frameworks, to a single, cohesive, consumer and innovation focused framework, within which specific sectoral initiatives can be incorporated.

Expansion of the Smart Data Framework into Other Priority Sectors

Whilst the initial Smart Data initiatives are being established, Government should look at ways to expand the broader framework with initiatives in other key sectors. When considering which sectors would be well placed for the introduction of a Smart Data Initiative, Government should begin by understanding which sectors potentially offer consumers and businesses the most opportunity for benefit through the ability to control and share their data. Such an assessment should look at what additional value could be released to consumers (either directly, or through potential new products and services), what value the 'holders' of the data currently derive from it (e.g. in relation to advertising), and the degrees to which the data is in a format that could be readily made available.

Based on these criteria, Barclays believes that Government should consider the introduction of a Smart Data Initiative in the online digital platform and technology sector (including social media, online commerce and other related platforms), which contains firms with some of the largest repositories of consumer and small business data. In addition, Barclays believes a comprehensive Smart Data Framework should enable consumers and businesses to more easily access and share their data held by public sector organisations, for example, tax and social security contributions. Government should therefore consider how public sector organisations could be effectively incorporated into the Framework.

Ultimately, we believe this proposed Smart Data Framework could provide the foundations to develop a comprehensive, Open Data economy enabling data portability for consumers and businesses across all sectors.

Raw Data Vs Elaborated Insight

Barclays considers it important that in any UK data sharing framework, policymakers consider the distinction between raw data and elaborated/inferred data insights. While consumers may have the right to control and access their raw and observed data (e.g. their transactions history), organisations often use their expertise and capabilities to build on this data to develop inferred data insights. These inferred data insights could be considered proprietary to an organisation and can have inherent value, although data subject rights will still apply to insights specific to an individual. In order to continue to encourage research, development and innovation, organisations must be able to retain this value. Further, this data is unique to an individual firms' processes, and would not necessarily be easily standardised or understood by other industry participants. It is for these reasons that Barclays does not believe inferred data insights should be subject to any data sharing frameworks.

Updating the UK Data Protection Framework to Support Innovation

The EU GDPR, and the UK's Data Protection Act have provided a world-leading data protection framework that empowers citizens, and places them firmly in control of their data and how it can be used by firms. These frameworks are undoubtedly positive in that they ensure consumers' data is protected, and their privacy is respected.

However, in an increasingly digital economy with vast volumes of data, it is the ability to access and use data that generates value and creates competitive advantage for firms. With the development of innovative technologies such as AI, Machine Learning, and DLT, firms are increasingly looking to experiment to explore how they could leverage such technologies to transform their businesses.

Unfortunately, there is currently a lack of clarity as to how to comply with the data protection framework when using these technologies, which risks deterring some firms from doing so. While ensuring that the UK does not significantly diverge from GDPR, Barclays believes there is a need to review the data protection framework in the UK, to provide greater certainty and clarity as to how data should be treated in the context of these technologies. Such action is required urgently to facilitate experimentation and innovation in the UK.

We provide a number of examples below, where greater clarity would be beneficial.

- **Blockchain**: one of the key characteristics of blockchain technology is that records are immutable i.e. data in a blockchain cannot be altered. Against the context of Article 17 of GDPR (the right of erasure/right to be forgotten) it is unclear how firms can comply with requirements to delete personal data if it were to be stored on chain. Whilst off-chain storage or encryption may provide 'work-around' solutions, Barclays believes Government should provide clarity as to how the Article 17 requirement for erasure can be achieved when using personal data and blockchain technology.

- **AI Experimentation**: both the purpose limitation principle and the data minimisation principle of GDPR make it difficult for firms to obtain consent of the data subject for the use of their personal data for AI experimentation. For instance, the purpose limitation principle makes it challenging to rely on the validity of any consent given. In addition, the data minimisation principle requires anonymisation or deletion of all data that is not necessary (with the term 'necessity' interpreted narrowly) for the specific purpose for which it was collected. Barclays believes Government should therefore provide guidance as to how firms should approach the issue of consumer consent in the context of AI experimentation.

- **The Use of Synthetic/Anonymised Data in AI**: Barclays believe further clarity is required regarding the point at which data is no longer able to be traced back to the data subject and therefore is not covered by GDPR.

- '**Data Controller' and 'Data Processor'**: Current data protection laws rely on a distinction between 'data controllers' (who determine the purposes and/or means by which personal data should be processed) and 'data processors' (those who process data only under instruction and on behalf of a data controller), that is based on outdated models of technology operations. Recent decisions by the European Court of Justice (ECJ) have highlighted some of the limitations of trying to apply these concepts to modern technologies. For example, large-scale cloud providers, who play an increasingly important role in the provision of financial market infrastructure, will often refuse to be bound, creating risks for financial services organisations who want to make greater use of cloud-based technologies, both for the commercial benefits they offer, but also in order to meet various regulatory obligations e.g. operational resilience requirements. Government should review the UK data protection framework to consider where rules may require updating to better reflect the use of cloud technology, and consider how responsibilities and obligations should be apportioned between providers.

- **Interplay Between Obligations Under Data Protection Legislation, Other Statutory Requirements and Common Law**: In certain fields, such as in financial services and health, there is a complex interplay between obligations arising under data protection laws, under other statutory regimes and under common law, such as obligations of confidentiality. There may be an opportunity to clarify the interaction between concepts arising under each framework, to provide greater certainty for organisations in understanding when they are able to share data, helping them to unlock potential benefits.

- **Promoting Privacy Enhancing Technologies**: Alongside reform to the legislation, Government should consider ways to promote Privacy Enhancing Technologies – technologies that enable data to be used and shared while maintaining privacy, for example pseudonymisation. Privacy Enhancing Technologies can play an important role in supporting the responsible use of data, helping to provide measures that allow for data to be re-used for research purposes, whilst ensuring individuals' rights remain protected.

- **Regulatory Interaction**: Many UK organisations are already subject to complex, sometimes overlapping regulatory regimes. For example, in addition to interaction between data protection (ICO) and sectoral regulators (such as the Financial Conduct Authority, Prudential Regulation Authority and OFCOM), there is also increasingly interest in data protection matters from the Competition and Markets Authority. The position is complicated further for organisations operating in multiple jurisdictions, who, in a breach scenario, may need to inform a number of regulatory authorities within particular timeframes, with complicated questions about sequencing. Aside from operational complexity, overlapping regulatory competence can lead to situations where it is unclear how competing requirements interact, or even where requirements appear to conflict. In the latter scenario, organisations are sometimes forced to choose which regulation to comply with. Though there is already some level of co-operation between regulators, there may be some benefit in clarifying the rules of engagement between regulators with competence for data protection and digital matters – in particular, when they are issuing guidance or introducing new requirements, and in matters of enforcement.

- **Consent Revocation**: it is important that users remain in control of their data, after they have provided consent for it to be accessed. Barclays believes further measures could be considered to ensure this is the case. For example: a requirement for clear and accessible documentation on how data is controlled, implementing proactive controls to manage access in order to maintain user trust, implementing proper controls for revocation and lineage management (in the case of data compromise) and the need for clear management of end of life access (managing access in case of data revocation).

Protecting the International Flow of Data

In today's global economy, many international firms have a presence or use suppliers located in jurisdictions across the world, requiring data to be transferred between jurisdictions. In order to protect this flow of data between jurisdictions, it is vital that effective mechanisms exist to enable firms to legally and efficiently transfer data across international borders, while ensuring data is safeguarded.

The Importance of an EU Adequacy Assessment

Barclays supports the Government's primary objective to secure and maintain an adequacy decision by the Commission under Article 45 of the GDPR. While Government likely appreciates the critical importance of a positive adequacy assessment to UK industry, we would further highlight that adequacy is by far the simplest, most efficient, and least burdensome solution to enable international data transfers to the EU. We would note that failure to obtain a positive adequacy assessment would likely create significant cost, disruption and administrative burden for many firms forced to implement alternative solutions. Further, a negative adequacy assessment would likely have further significant implications for positive due diligence assessments required for the use of Standard Contractual Clauses (SCCs) to transfer data from the EU to the UK following the ECJ's Schrems II ruling.

Barclays also supports the decision taken by the Government to deem the EU adequate under the UK framework, permitting the transfer of data from the UK to the EU.

Notwithstanding any finding the Commission may make in respect of UK adequacy, we would expect that Government will of course in any case need to continue to work closely with the relevant EU parties towards a pragmatic interpretation of EU rules that concern data and the digital economy so as to provide certainty for organisations operating in both the UK and EU, and minimise the potential for regulatory divergence on these issues.

Data Transfers Beyond the EU

Beyond adequacy with the EU (and the EEA), we would encourage the Government to seek reciprocal data transfer arrangements with other major jurisdictions around the world. Firstly, we support the Government's intention set out in the Strategy to review data transfer frameworks of jurisdictions deemed adequate by the EU. Beyond those jurisdictions, Barclays would specifically highlight the importance of data flows from the UK to India, the US and Singapore.

- **India** - any initiatives that facilitate date transfers to India, whether they be codes of conduct, bilateral agreements, or adequacy decisions, would be welcome. While India may not currently have in place a legal framework that would satisfy UK standards of data protection, we would note that it is in the process of introducing its own Data Protection framework. While this is positive there is a risk that certain provisions may require data to be stored in India / prevent data being transferred back to the UK. We would encourage the Government to engage with the relevant Indian authorities to ensure data sent to India but not covering Indian citizens is permitted to be transferred back to the UK.
- **Singapore** - Singapore already has a relatively well-developed data protection regime, so a reciprocal agreement permitting data transfers should be achievable.
- **The US** – given the significance of the UK–US relationship, an agreement permitting the free flow of data would be welcome. However, the current approach to data protection in the US (i.e. the lack of a national framework, and federal regulator) could create challenges and potentially have knock implications for agreements with the EU. It is important that the UK does not overly relax data protection standards to achieve a data transfer arrangement with the US, as this could serve to prevent an adequacy assessment from the EU.

Other key jurisdictions that Government should prioritise for data transfer agreements include: those with established regulators and frameworks similar to the UK framework, e.g. Australia, Canada, New Zealand, Japan. Further, we suggest other major jurisdictions for prioritisation could be: Switzerland, South Africa, Brazil and Hong Kong. While agreements with these jurisdictions would be positive, it is important that Government assesses their frameworks carefully and seeks to achieve enhancements when necessary, to ensure effective protection of UK personal data. This may be particularly relevant for the US and Hong Kong.

While the Strategy notes the potential to agree an adequacy decision for a particular 'territory' within a jurisdiction, these may add an extra level of complexity and so country level decisions should be sought wherever possible. Where recognition at the territory or jurisdictional level is not possible, Government may wish to consider the feasibility of 'sectoral' adequacy decisions for sectors that rely on the ability to transfer large volumes of data internationally. Many organisations will already be subject to comprehensive requirements from sectoral regulators, ensuring oversight of outsourcing arrangements, the security of systems and operational resilience. These rules may provide the basis

for sectoral adequacy decisions, or the foundations for sector specific frameworks to be developed in future.

Alignment with International Standards

It is worth noting that since its introduction, many countries around the world have aligned their legislation to GDPR, either with the objective of ensuring or preserving an adequacy decision, or in recognition of GDPR as the embodiment of current best practice. As continued alignment with GDPR could enable agreements with other jurisdictions that seek to emulate GDPR, we would caution the Government against any significant divergence of UK data protection law from the standards enshrined by GDPR. A significant divergence in the UK risks creating multiple frameworks for global firms to comply with, and if divergence creates a softer regime, could result in the UK failing to achieve key adequacy decisions.

Rather, we support the Government's intention to collaborate with international stakeholders, and would encourage the Government to lead discussions in this area to agree common, high standards for data protection that can enable mutual recognition of frameworks between jurisdictions. As part of this role, Barclays would strongly support Government efforts to prevent the use of unjustified data localisation measures which create significant disruption and cost to the global data economy. Specifically, Government should continue to ensure bilateral trade agreements do not allow for such measures, and should look to drive engagement on this issue through supra-national bodies such as the OECD. For instance, Government may wish to consider whether the forthcoming British presidency of the G7 should continue the work of the US G7 presidency considering cross-border data issues for financial services organisations.

Data Transfer Mechanisms

Beyond the data adequacy framework, the UK should look to maintain and develop the current range of alternative data transfer mechanisms available that provide flexibility and legal certainty.

In particular, we would encourage the development of processor to processor standard contractual clauses (P2P SCCs), which would allow UK-based processors to share data lawfully with sub-processors based outside of the jurisdictions recognised as adequate by the UK. We note that the European Commission currently has a consultation on a set of P2P SCCs, so any similar UK initiatives would need to take that into account. Further The development and introduction of approved international transfer codes of conduct and certification schemes would be welcomed and would enhance flexibility.

Regarding the use of Binding Contractual Rules (BCR), we would note that the current process of developing and agreeing BCRs can be onerous for organisations to undertake, can take significant time to complete. We would also flag a practical constraint in the existing approval process, in that the number of applications that can be processed by resource at the ICO is limited. We would encourage Government to consider whether there may be opportunities to make this process more agile, and whether there may be some role for self-certification.

We also note that some of the existing mechanisms permitted for under legislation may be under-utilised. Codes of Conduct, for instance, could provide a useful tool for demonstrating compliance, but appear to have been hampered by procedural issues around their approval, as well as a lack of

clarity around ensuring oversight of these. Clarification and streamlining of the approval process for adoption and oversight of Codes of Conduct, along with working with organisations and trade bodies to promote the benefit of these, could provide an immediate benefit for UK organisations.