U.S.-UK
Business Council

December 2020

Response to the UK National Data Strategy Consultation

The U.S. Chamber of Commerce ("Chamber") is the world's largest business federation, representing the interests of more than three million enterprises of all sizes and sectors. The Chamber is a longtime advocate for strong commercial ties between the United States and the United Kingdom. Indeed, the Chamber established the U.S.-UK Business Council in 2016 to help U.S. firms navigate the challenges and opportunities from the UK's departure from the European Union as well as to represent the views of business as the U.S. and UK negotiate a new trade agreement. With over 40 U.S. and UK firms as active members, the U.S.-UK Business Council is the premier Washington-based advocacy organization dedicated to strengthening the commercial relationship between the U.S. and the UK.

According to a recent U.S. Chamber study, U.S. and UK companies have together invested over $1.3 trillion in each other's economies, directly creating over 2.75 million British and American jobs.[1] We are each other's single largest foreign investors, and the U.S. is the UK's largest trading partner.

The Chamber is also a leading business voice on digital economy policy, including on issues of data privacy, cross-border data flows, cybersecurity, digital trade, artificial intelligence, and e-commerce. In the U.S. and globally, we support sound policy frameworks that promote data protection, support economic growth, and foster innovation.[2]

The Chamber's U.S.-UK Business Council welcomes the opportunity to provide Her Majesty's Government ("HMG") with comments on its National Data Strategy ("Strategy"). We welcome further opportunities to discuss this input with colleagues from DCMS and other UK Government agencies as this Strategy is implemented in the weeks and months ahead.

[1] U.S. Chamber of Commerce, The Transatlantic Economy 2020.
[2] U.S. Chamber of Commerce, Data Privacy.

Overall Questions

Q1. To what extent do you agree with the following statement: Taken as a whole, the missions and pillars of the National Data Strategy focus on the right priorities. Please explain your answer here, including any areas you think the government should explore in further depth.

- **Strongly disagree**
- **Somewhat disagree**
- **Neither agree nor disagree**
- **Somewhat agree**
- [✓ **Strongly agree**]

The Chamber applauds the UK Government's proactive focus on the importance of data-driven innovation, including cross-border data transfers which underpin the modern economy across all sectors, for companies of all sizes. In addition, we welcome the Strategy's focus on making more government data publicly available and accessible. As the UK leaves the EU single market and customs union, there are additional opportunities to expand its leadership in data policy and digital trade, as exemplified in the recent *UK-Japan Comprehensive Economic Partnership Agreement*, which includes state-of-the-art disciplines critical for the UK's growing digital economy.

Harnessing the potential of data will require a British workforce with the necessary skills to collect, maintain, analyze, and apply data. For example, the UK's National Health Service will need staff with the expertise to collect data accurately, the time to do it, an understanding of how this data improves patient outcomes, increases the overall efficiency of the health service, and supports research into new medicines and treatments. Data and digital skills are increasingly important to innovation across the economy. For the UK to remain competitive, the Government and its Data Strategy needs to focus on the tools needed to ensure the development of strong data science skills across the workforce.

Q2. We are interested in examples of how data was or should have been used to deliver public benefits during the coronavirus (COVID-19) pandemic, beyond its use directly in health and social care. Please give any examples that you can, including what, if anything, central government could do to build or develop them further.

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.

Digital services and cross-border data transfers have allowed much of the economy to remain connected and maintain high levels of productivity, in spite of the lockdowns, strains on essential services, and restrictions on movement. This remarkable evolution, implemented almost overnight, has transformed our economies and underscores the importance of data. The new economic reality has also reemphasized the importance of ensuring our workforces are well-educated and have the digital skills necessary to succeed, including the ability to adapt to remote working environments.

Data has also underpinned the economic response to the pandemic. Public service authorities have been able to use and analyze data to quickly understand where economic needs have been greatest, to provide essential services remotely, and distribute financial assistance. There are also countless examples of local, regional, and international logistics and transportation companies and agencies reconfiguring and streamlining their networks and frequencies in accordance with the data they've collected throughout the pandemic.

Mission One: Unlocking the value of data across the economy

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.

Q6. What role do you think central government should have in enabling better availability of data across the wider economy?

The Chamber encourages HMG to provide additional opportunities for companies and individuals to access and use government data, provide legal clarity for the pooling of data undertaken by private sector organizations, and encourage voluntary data sharing between governments and businesses as well as between businesses.

We discourage mandatory data sharing requirements for private sector actors, as these policies undermine market competition, deter innovation and investment, and violate intellectual property rights.

By contrast, encouraging sharing of public sector data and voluntary data sharing between companies (for example health research data that can be analyzed by multiple firms as they work to combat the COVID-19 pandemic) are laudable goals that should be encouraged by the National Data Strategy.

HMG should work closely with industry and other stakeholders to identify the sectors that would benefit most from increased sharing opportunities. Further, the Government should work closely with stakeholders to identify the legal and financial incentives it is prepared to endorse in order to encourage the voluntary sharing of private sector data, as well as remove potential barriers.

Q6a. How should this role vary across sectors and applications?

In order to maximize the benefits of data availability across the economy, the UK Government must work closely with sectoral regulators and the private sector to consider how existing rules promote or hinder voluntary data sharing and the usage of open government data. The approach to expanded availability must be tailored to the needs and specific circumstances of different sectors and agencies. A "one size fits all" approach to data availability, sharing, and access may not work.

Data foundations: The true value of data can only be fully realised when it is fit for purpose, recorded in standardised formats on modern, future-proof systems and held in a condition that means it is findable, accessible, interoperable and reusable. By improving the quality of the data we are using, we can use it more effectively, and drive better insights and outcomes from its use.

Q7. To what extent do you agree with the following statement: The government has a role in supporting data foundations in the wider economy. Please explain your answer. If applicable, please indicate what you think the government's enhanced role should be.

- **Strongly disagree**
- **Somewhat disagree**
- **Neither agree nor disagree**
- **Somewhat agree**

- **Strongly agree**

"Data foundations" are rightly identified as a core pillar of the strategy. However, there are several barriers currently undermining the UK's data foundations where Government investments and actions are needed. It is important that the right tools and systems are in place to support consistent collection, storage and management of data, as well as maximizing the interoperability of existing datasets.

HMG should take care to work closely with industry stakeholders and other interested parties to ensure that these standards are voluntary, open, technology-neutral, and interoperable with other international standards to ensure their effectiveness. Creating UK-specific models of governance or new standards systems would undermine the ability of firms, governments, and individuals to make full use of the newly available and accessible data.

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?

The UK Government should take care to ensure that the rules of the road for data governance are clear, flexible, and scalable to fit the needs of companies of all sizes. Governments sometimes erect unintentional barriers to voluntary data sharing, international data transfers, or to access to public data, be it through overly burdensome data privacy or cybersecurity requirements. Policymakers need to consider how this may disproportionately impact small and medium-sized enterprises, which cannot absorb legal costs or handle administrative burdens in the same manner as larger companies.

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

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

Ensuring a data protection framework that is reliable, predictable, and compatible with the realities of the interconnected global economy is essential. After the UK fully leaves the EU single market and customs union at the end of 2020 there is a unique opportunity to demonstrate international leadership in this area and improve the business climate for companies operating in the UK.

The UK should consider ways it can streamline the application of the Data Protection Act in a manner that advances a risk-based approach to data privacy. One area could be in expanding the circumstances in which a company can choose to use the "legitimate interest" basis for processing personal information. Efforts by data protection authorities, both in the UK and in the EU to narrow the legitimate interest basis for collecting and processing data, which requires enterprises to undertake a risk-based balancing of interests, run counter to such an approach. Another area to consider is the 72-hour breach notification rule inherited from GDPR, which currently incentivizes over-notification, and whose threshold can be made more flexible. At the same time, reforms to the Data Protection Act should be weighed against the need to maintain alignment with the European Union for the purposes of securing and maintaining an adequacy decision.

Separately, the Chamber cautions the UK Government against instituting changes to the Data Protection Act to enable representative legal actions. We call attention to our comments to DCMS's recent consultation (submitted on October 28th by the U.S. Chamber of Commerce's Institute for Legal Reform), outlining our recommendations and specific concerns.

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

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

- **Quality, availability and access**
- **Standards and assurance**
- **Capability, leadership and culture**
- **Accountability and productivity**
- **Ethics and public trust**

We want to hear your views on any actions you think will have the biggest impact for transforming government's use of data.

Increasing the public availability of government data—and promoting a culture of data openness—are keys to promoting innovation and ensuring maximum positive impact. We applaud the UK government's efforts to demonstrate international leadership in this area, both domestically and internationally including through next year's G7 presidency and the ongoing work of the Digital Nations group.

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. We welcome your views on standards that should be prioritised, building on the standards which have already been recommended.

Governments should work to advance important standards policy in support of open and competitive markets. The development of global standards in close, active, ongoing collaboration with the private sector is the best way to promote common approaches that are both technically sound and deliver technology-based solutions and policy objectives. Such standards should be voluntary, open, transparent, globally recognized, consensus-based, and technology-neutral. These efforts should build upon the international standards principles established by the World Trade Organization's Technical Barrier to Trade Agreement by promoting the alignment of standards across borders, facilitating trade in connected products, and stimulating innovation in industry.

Mission Four: Ensuring the Security and Resilience of the Infrastructure on which data relies

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?

The Security of Network and Information Systems Regulations (NIS Regulations) adopted by the UK Government in 2018 provide legal measures and baseline cybersecurity for both operators of essential services and digital services providers. These measures provide guidance to national competent authorities and sector specific agencies based on internationally recognized security standards and frameworks (e.g., ISO/IEC 27001, U.S. National Institute of Standards and Technology Cybersecurity Framework). As appropriate to the risk in an evolving threat landscape, competent authorities should conduct public consultations and host stakeholder engagement sessions to evaluate the effectiveness of these risk management programs, processes, and standards. To the extent that any gaps or deficiencies are identified, the Chamber urges HMG to ensure that enhanced measured are aligned with international measures and are scalable such that they might be interoperable in other jurisdictions.

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?

Clients assess the robustness of security protocols through a variety of different, and oftentimes layered, third-party risk managements (TPRM) means. Frequently, security questionnaires accompany TPRM processes, however, these qualitative assessments are just one part of many organizations' efforts to manage risk.

The Chamber urges organizations to (1) build a framework for third-party categorization, (2) develop a workflow to address the intersection of risk and criticality, (3) establish a cadence for frequent assessment of high-impact suppliers, and (4) ensure appropriate risk transfer. While the Chamber endorses technology neutral approaches to risk management, we have observed the market reward organizations that invest in a number of TPRM tools, for example, cybersecurity insurance, penetration testing, identity and access management, and security ratings to name a few.

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, data service providers, their supply chain and their clients?

The Chamber urges governments to set a clear public policy direction that the use of data service providers, such as cloud computing (e.g., infrastructure, platform, communications, software), is beneficial to national and economic security and a key enabler for the broader digital economy. A sound policy framework that underscores the importance of security, privacy, trust, and transparency is also important to the growth of the market for data service providers. Global benchmarks and best practices illustrate that cross-border data flows complement and effectuate these public policy aims. The Chamber recommends that future UK Government frameworks explicitly recognize this relationship between data flows, security, and resilience.

With regard to security and resilience standards, private industry greatly benefits when governments incorporate existing cybersecurity frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework or the International Organization/International Electrotechnical Commission (ISO/IEC) 27001:2013, into any future policy enactments and avoid mandating local standards and requirements that diverge from these international norms. These frameworks are largely process-focused—designed to help organizations start a cybersecurity program or improve an existing one—and are applicable to cloud computing environments. There are several cloud specific security standards initiatives that have recently been published, including ISO/IEC 27017 and ISO/IEC 27018, that provide more detailed guidance and recommendations for both cloud service customers and cloud service providers.

Q16. What are the most important risk factors in managing the security and resilience of the infrastructure on which data use relies? For example, the physical security of sites, the geographic location where data is stored, the diversity and actors in the market and supply chains, or other factors.

Risk factors vary across industries and organizations. Recently, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) published a report, Lessons Learned During the COVID-19 Pandemic, which might offer a few insights into supply chain risk management.[3] Among the numerous recommendations is one to reduce the risk of single source and single region suppliers. Also, organizations should be encouraged to build a framework for third-party categorization whereby critical junior-tier suppliers are identified. To the extent possible, organizations should leverage multiple suppliers to provide essential critical functions such that the organization isn't completely dependent on a single source.

Q17. Do you agree that the government should play a greater role in ensuring that data does not negatively contribute to carbon usage? Please explain your answer. If applicable, please indicate how the government can effectively ensure that data does not negatively contribute to carbon usage.

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- [✓ Somewhat agree]
- Strongly agree

Technology companies and data centers are at the forefront of the environmental and sustainability transition. Digital connectivity allows for increased capacity and

[3] U.S. Cybersecurity and Infrastructure Security Agency, Lessons Learned During the COVID-19 Pandemic

productivity from remote working environments, lessening the strain on infrastructure and transportation systems—and lowering emissions.

The free flow of data across borders prevents the need for building, maintaining, and powering duplicative data centers in many different locations. Connectivity to the cloud powered by these data centers also improves the accessibility of data for both governments and companies who depend on these services. Data centers are increasingly powered by renewable energy—primarily solar and wind. Cloud services providers are committed to doing their part to reducing carbon emissions and reducing the harmful impacts of climate change.

We encourage HMG's approach to the green transition—as well as the digitalization of the UK economy—and look forward to opportunities for active, ongoing stakeholder engagement as these policies develop. International investors, including from the information technology sector, are eager to be involved in these discussions.

Mission Five: Championing the International Flow of Data

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

We will seek EU 'data adequacy' to maintain the free flow of personal data from the EEA and we will pursue UK 'data adequacy' with global partners to promote the free flow of data to and from the UK and ensure it will be properly protected.

As the UK sets out its own independent trade and data protection framework, it has an opportunity to upgrade the adequacy process "inherited" from the European Union by making it more consultative, transparent, predictable, and outcomes focused. The existing EU process is severely lacking on all of these fronts: there is minimal opportunity for stakeholder engagement and feedback, the process is opaque and time-intensive, adequacy can be withdrawn at any time , with no guaranteed transition period for companies, and the primary means of achieving adequacy is to essentially copy and paste the European legislation. The UK can, and must, do better.

We are already encouraged by the o the UK's early commitment to the free flow of data across borders and to digital trade, as outlined in the final text of the UK-Japan trade agreement. The Chamber appreciates that the disciplines on data flows go well beyond the status quo and that the bans on data localization measures extend to all sectors of the economy. We hope HMG will continue to prioritize these measures in its future trade agreements, including with the United States, as well as in plurilateral fora.

Q19. What are your views on future UK data adequacy arrangements (e.g. which countries are priorities) and how can the UK work with stakeholders to ensure the best possible outcome for the UK?

Given the close trade and investment ties between our countries—all of which is underpinned by the transfer of data—a first priority must be identifying additional means to promote data transfers between the UK and the United States. While the European Court of Justice has declared the existing EU-U.S. Privacy Shield mechanism invalid, the UK has the opportunity to clarify the rules surrounding transfers of personal information with its largest single country trading partner and single largest foreign investor. We encourage DCMS, in partnership with the private sector, to explore new ways for enabling U.S.-UK data flows, including through the exploration of sectoral adequacy decisions, interoperability with existing mechanisms such as the Asia-Pacific Economic Cooperation's *Cross-Border Privacy Rules System,* and voluntary certifications and codes of conduct.

Conclusion

The U.S. Chamber of Commerce's U.S.-UK Business Council appreciates the opportunity to provide these comments on the UK's National Data Strategy. We look forward to opportunities to collaborate and provide additional input as these policies continue to be developed and implemented.

Contact: Garrett Workman
Senior Director, U.S.-UK Business Council &
Senior Director, European Affairs, U.S. Chamber of Commerce
gworkman@uschamber.com
+1 (202) 503-7522