BSA | THE SOFTWARE ALLIANCE'S COMMENTS ON THE UNITED KINGDOM NATIONAL DATA STRATEGY

BSA | The Software Alliance ("BSA"),[1] the leading advocate for the global software industry, supports the UK's forward-looking efforts to build a modern economy driven by data and welcomes the opportunity to provide comments on the United Kingdom National Data Strategy.

Key BSA Recommendations

Overall recommendations:

- Support the uptake of digital technologies to leverage data and software tools to support businesses;
- Use data to enhance online trust and security;
- Further clarify priorities and governance for the future roll-out of the National Data Strategy.

Mission one: Unlocking the value of data across the economy

- Establish a policy framework that enhances access to high value government data, makes it easier for organizations to voluntarily share their own data, and promotes the development and use of privacy-enhancing technologies that enable data collaboration in ways that align with the public's expectation of privacy.

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

- Ensure that the UK's privacy framework remains outcome-driven and does not inadvertently stifle responsible and data-driven innovation and the competitiveness of UK firms;
- Maintain the UK international data flows regime so it allows for several options for seamless cross-border data flows across key jurisdictions for the UK economy;
- Preserve existing tools that have been widely adopted by the business community and recognize the power of issuing UK adequacy determinations to priority countries;
- Drive trust-based governance globally, including in fora such as the World Trade Organization Joint Statement Initiative on e-commerce.

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, Akamai, Atlassian, Autodesk, Bentley Systems, Box, Cadence, Cloudflare, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org

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

- Build a culture of internal data sharing and accessibility within Government;
- Consider developing a simple risk-based framework based on appropriate compliance and legal controls;
- Facilitate consistent data collection practices should be put in place for better data quality and productivity benefits in the administration.

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

- Support Cloud infrastructure security policies that prioritize a risk-based, technology-neutral, adaptable approach in the systems and services that store, process and transfer data;
- Regulatory obligations should treat cloud computing in a similar way as other types of outsourcing, recognizing that both the cloud provider and its customer share security responsibilities;
- Enable Government to play a role in relevant aspects of ensuring security, continuity and resilience of service for cloud infrastructure providers;

Mission five: Championing the international flow of data

- Strive to play a thought-leadership role as the global conversation on multilateral digital trade rules and convergence of privacy regimes continues;
- Prioritize the interoperability of the UK Privacy Act transfer mechanisms with other mechanisms used in leading global privacy frameworks;
- Continue to work towards modern digital trade provisions in its bilateral and plurilateral agreements as a way to support its digital economy.

Detailed BSA Responses

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**

BSA agrees that the National Data Strategy includes the right missions and pillars. The Strategy is an ambitious set of measures and we would welcome additional clarity on two important areas: priorities and governance. We would welcome a work plan with priority actions to be taken forward and the establishment of a body responsible for coordinating the rollout of the Strategy between Government departments. This governing body should also include industry stakeholders who are involved in turning this Data Strategy into reality.

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.

Data plays a critical part in addressing immediate challenges raised by the pandemic, support short- and mid-term recovery, and enable long-term growth and prosperity. In fact, the value of data extends far beyond responding to public health crises. Collaboration around "open data"–i.e., non-sensitive government data that is made freely available to the public in non-proprietary, machine readable formats via non-restrictive licenses–can unlock opportunities that spark the economy and fuel job growth in virtually every industry sector.

From healthcare and manufacturing to agriculture and retail, software-powered digital technologies are becoming an integral part of how companies design, create, and export new products and services; enhance business processes and increase productivity; reach new customers; manage their supply-chain and engage in research and development. The COVID-19 pandemic has accelerated this digital transformation by forcing many aspects of public life to a remote environment—be it work, health services, or learning—further highlighting the importance of the digital economy and the benefits of digital transformation for governments, companies, and citizens.

Support the uptake of digital technologies to leverage data and software tools to support businesses. Central government should support the uptake of these technologies to leverage data and software tools to support businesses. Businesses increasingly use data-driven software tools and cloud services to support essential business functions, such as managing payrolls, sustaining e-commerce, training employees, and ensuring the resilience of supply chains. In 2018, 30% of UK companies had integrated

some form of cloud computing solutions, compared to an average of 18% in the European Union.[2] Digital technologies also help modernize sectors that have to date been slow to adopt technological innovations and in so doing can improve their delivery of products and services.

- For example, data can feed into analytics tools that examine past product demand, and AI algorithms can be trained to use that information combined with other data points to predict future demand. Companies can get insight into local and global trends that can help them better manage their businesses.[3]
- Health and social care data can also be used beyond the medical and research world and provide valuable information to other sectors such as financial services. For example, life insurance companies can capture real-time hospitalization, infection, and death related data from public health organizations for analysis with traditional demographic and claims data. This allows them to improve how they forecast the financial impact of life insurance claims from policy beneficiaries, while at the same time offering new services to those beneficiaries to become new clients.[4]

Use data to enhance online trust and security. The pandemic and related transition to a largely remote economy have also created an opportunity that malicious actors have been exploiting, leading to a surge in online scams and cyber-attacks.[5] Trust and security should be integral component of a data-driven economy. Data can be used to monitor the threat landscape and when shared, can provide valuable information to help organizations maintain and adapt their cyber security posture.

Against this background and in addition to recommendations detailed in this submission, BSA recommends that the UK Government:

- Support the uptake of digital technologies to leverage data and software tools to support businesses;
- Use data to enhance online trust and security.

Mission one: Unlocking the value of data across the economy

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

Access to data, as the Data Strategy states, is key to UK's economic recovery from COVID-19, and to supporting job creation and efficiency gains across all sectors. Ensuring that quality data is available and

[2] UK country Profile, EU Digital Economy and Society Index 2020 https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66933

[3] Adobe Digital Economy Index: "Tracking the State of Ecommerce During COVID-19 and Beyond," Adobe Blog, March 2020 https://blog.adobe.com/en/2020/03/31/adobe-digital-economy-index-tracking-the-state-of-ecommerce-during-covid-19-and-beyond.html#gs.ir0fj4

[4] "COVID-19's Impact on Data Governance and Risk Management Across Financial Services" Informatica Blog, July 2020 https://blogs.informatica.com/2020/07/17/covid-19s-impact-on-data-governance-and-risk-management-across-financial-services/

[5] "Advisory: COVID-19 exploited by malicious cyber actors," UK NCSC, April 2020 https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory. See also "Digital security risk is increasing as the coronavirus (COVID-19) crisis unfolds," OECD, April 2020 http://www.oecd.org/coronavirus/policy-responses/dealing-with-digital-security-risk-during-the-coronavirus-covid-19-crisis-c9d3fe8e/

accessible is key to helping businesses develop innovative business practices as well as new products, tools and solutions that can be deployed across the country.
Three areas should require particular attention:

- First, data can only have the most impact if it is properly identified. However, a majority of organizations report that more than half of their data is 'dark,' meaning it's unknown or untapped.[6] Operational efficiencies can be achieved, and possibly unknown opportunities can be identified, if appropriate data analytics tools and solutions are used to that effect and government support would be helpful;
- The Government should adopt a consistent strategy of making more data available across the economy, irrespective of the type of data at hand. In the enterprise context, data comes in various, sometimes cumulative, categories, primarily: operational data generated by machine processes, non-personal data and personal data, structured and unstructured data. The nature of the data is an important determination to set the right framework for protecting, processing and sharing data. The strategy should take into account the specificities that pertain to each category;
- Finally, the Government has a role to play in educating industrial sectors about data use. Productivity increases have been very low in the UK since the 2008 financial crisis and the UK could address this 'productivity puzzle' by investing in human capital and educating the workforce about the benefits of data-driven solutions for industrial sectors.

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

Data is the lifeblood of the modern digital economy – powering innovation, spurring economic growth, and enabling organizations to create new jobs, boost efficiency, drive quality, and improve output.

To unlock the value of data across the economy, the UK should establish a policy framework that:

1) enhances access to high value government data,
2) makes it easier for organizations to voluntarily share their own data, and
3) promotes the development and use of privacy-enhancing technologies that enable data collaboration in ways that align with the public's expectation of privacy.

Enhancing Access to Government Data and Public Sector Information.
Government-generated data is a resource that can serve as a powerful engine for creating new jobs and promoting economic growth. At both the local and national level, agencies collect and generate vast quantities of data that offer unique insights into virtually every facet of the modern world, from satellite imagery that can help predict the weather to transportation data that can help reduce congestion.
The Data Strategy should build on this ensure that the UK has the right policies, infrastructure, and resources in place to enhance access to government data. To that end, BSA recommends:

- Establish an Open Data Legislative Framework: The UK has long been a leader in prioritizing the availability of government data and has embraced a commitment to making government data "open by default."[7] As part of the Data Strategy, the UK should codify its open data commitments. As the past few months have demonstrated, ensuring that the public has access to trustworthy

[6] Splunk Data Data report, 2019, https://www.splunk.com/pdfs/dark-data/the-state-of-dark-data-report.pdf
[7] https://www.gov.uk/government/publications/uk-digital-strategy/7-data-unlocking-the-power-of-data-in-the-uk-economy-and-improving-public-confidence-in-its-use#fn:1

and dependable data can be a matter of life and death. Throughout the COVID-19 pandemic, scientists and policymakers have used open data to learn more about the virus and plan effective responses to it, examining everything from mobile phone mobility data to information about health system capacities. Open case count and new infection rate data has been a critical tool in slowing the spread of the virus, and as we inch closer to an effective vaccine, ensuring that researchers can collaborate around and share datasets will remain a top priority. COVID-19 has also illustrated the critical importance of ensuring that our institutions rest on solid legal foundations, that they are backed by adequate resources, and that this groundwork has been laid in advance of an emergency. Codifying the United Kingdom's strong open data policies will help achieve these objectives.

- Appoint a National Chief Data Officer: Ensuring that data is collected, maintained, and shared in ways that maximize its value is a complex task that requires dedicated senior leadership. A national Chief Data Officer can help establish consistent and effective data governance practices across government agencies and help to ensure that data resources are being fully leveraged across departments. Although agency CDOs will help maximize the value of data within each individual agency, ensuring whole-of-government interoperability will require a consistent approach to data governance.
- Establish an Open Data Advisory Council: The UK should establish a public-private advisory council to provide recommendations to the CDO about data that would be most impactful to the public, industry, and government. By bringing together experts from within government, industry, and civil society, such a council will enhance the return on investment of open data policies by creating a mechanism for ensuring that government data is "published with purpose" and that agencies are prioritizing the release of data assets with the greatest potential for positive impact.
- Modernize IT Infrastructure to Support Open Data: Delivering on the Data Strategy's vision for leveraging government data as a strategic asset will ultimately depend on whether government agencies have the resources and infrastructure they need to make effective use of data. Reliance on aging physical data centers can result in data siloes that prevent an agency from making use of data outside of the application the agency used to generate it, and make it exceedingly difficult to share with the public. Open data commitments should be supported by efforts to modernize the government's aging IT infrastructure through the adoption of commercial cloud offerings.

Promote Voluntary Industry Data Sharing. Across industries, there is growing recognition of the immense collective benefits that can arise when organizations share data in ways that facilitate collaboration.

- Establish Expedited Regulatory Review Processes: Despite growing recognition of the benefits of voluntary data sharing, a recent MIT study revealed that 64% of global business executives cite concerns about regulatory uncertainty as an impediment to fully embracing the benefits of open data.[8] To promote more robust industry data sharing, the UK should establish expedited review processes to enable relevant authorities to review and clear data sharing arrangements, consistent with competition and privacy considerations.
- Modernize the Copyright Act: The UK should modernize the Copyright Act to ensure that the research community and industry have the flexibilities that are necessary to perform analytics, including text and data mining, on any content to which they have lawful access. Specifically, the UK should broaden the current copyright exception on Text and Data mining, to bring it in line

[8] MIT Technology Review, *The Global AI Agenda*, https://bit.ly/GlobalAIagendaPDFENG

with global standards and to ensure that the UK is well placed to be at the forefront of data analytics.

- Promote the Development of Data Sharing Tools and Best Practices: The UK should support the development, availability, and adoption of tools and best practices that make it easier and less expensive to share data in ways that are consistent with rigorous privacy expectations. Technical tools, such as application programming interfaces (APIs), can facilitate data exchanges that are faster and more secure than traditional transfers. In addition to technical tools, it is important to promote the development and use of standardized data licensing models. Any new initiative should build on prior work done in this space by the UK in the form of its Open Government Licence for Public Sector Information.[9] Much as the development of standardized open source licenses gave rise to a new model for software innovation, standardized data license agreements can facilitate new collaborative approaches for sharing data resources. The Linux Community Data License Agreement[10] and the Open Use Data Agreement[11] are good examples of industry efforts to create tools that will democratize the value of data by making it easier for all stakeholders to voluntarily share data in a manner that is predictable and trustworthy.

Embrace Privacy-Enhancing Technologies. Improved access to data need not come at the expense of privacy. Indeed, a range of privacy-enhancing technologies and data governance structures can enable value-added uses of data without compromising the confidentiality or security of the underlying data. To that end, the UK should promote the use of privacy enhancing technologies – such as differential privacy, homomorphic encryption, and federated machine learning – to create opportunities for sharing data while preserving individual privacy. It should likewise support the development of innovative data governance structures – such as data trusts, data cooperatives, and data commons – that facilitate public and private sharing of data in ways that preserve privacy while enabling participants to benefit from the analysis of potentially sensitive data. Investments in R&D and the creation of regulatory sandboxes can also help spur the development of such arrangements.

- Leverage Privacy-Enhancing Technologies to Enable Cutting Edge Research: The UK should seek out opportunities to enable experimentation and collaboration on high-value data through the use of privacy-enhancing technologies. New analytic and data governance technologies can enable researchers to collaborate around shared data resources while preserving confidentiality. For instance, 30 leading hospitals recently launched a project to jointly train an AI system to assist radiologists in identifying early-stage brain tumors.[12] By leveraging "federated learning," the platform allows the system to be trained on each institution's data without exposing any individual patient's medical records. The UK should leverage such technologies to enable cutting-edge research on data that cannot be shared more openly.

[9] Open Government Licence for Public Sector Information, http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/

[10] The Linux Foundation Projects, Community Data License Agreement, https://cdla.io/

[11] Microsoft, The Open Use of Data Agreement, https://github.com/microsoft/Open-Use-of-Data-Agreement

[12] https://www.wsj.com/articles/intel-health-institutions-to-use-emerging-ai-technique-to-improve-tumor-detection-11589191200?mod=djemAIPro

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?

Trust and confidence must be a foundation of today's digital economy, which benefits companies of all sizes and across all industry sectors. Trust and confidence are the catalysts that will ensure that data and technology can reach their full potential in the betterment of society. The enterprise software industry is at the forefront of the development of cutting-edge innovation, including data analytics and artificial intelligence. Software-enabled technologies increasingly rely on data and, in some cases, personal data, to function to the benefit of business customers. As a result, the protection of personal data is an important priority for BSA members, and we recognize that it is a key part of building customer trust. As it reflects on its data protection framework and possibly further defines relevant policies and legislation, we recommend that the UK considers the following aspects:

Future-proof privacy in an ever-evolving technological landscape:
In an ever-evolving technological landscape, data privacy legislation must ensure that citizens' personal data is protected by strong safeguards, that organizations handling personal data have legal certainty and a range of tools to comply, while enabling them to seamlessly operate, grow and innovate.
The UK Data Protection Act 2018 implementing the General Data Protection Regulation (GDPR), includes important rights for consumers and obligations on businesses. It also includes provisions that impact the development and use of emerging technology such as Artificial Intelligence (AI) and machine-learning, which are critical to a range of industries in data-driven economies. For example, the Data Protection Act defines "personal data" broadly, as any information that directly or indirectly identifies or could be used to identify natural persons (Article 3(2) and 3(3)). This broad definition can capture data used to engineer and train AI systems, as well as data used by AI systems to generate predictions and make recommendations. The Data Protection Act also applies heightened protections to certain uses of personal data, such as use of biometric data, profiling, and automated decision-making without human intervention. It therefore comprehensively regulates the use of personal data, including in connection with the lifecycle of an AI tool that uses personal data, from inception to deployment.[13]

- Going forward, it will be important to ensure that the UK's privacy framework remains outcome-driven and does not inadvertently stifle responsible and data-driven innovation and the competitiveness of UK firms.

Privacy and the movement of data:
Data underpins the use of digital technologies by companies across all industries. A core foundation of digital transformation is the ability for data, including personal data, to move seamlessly across borders. Indeed, the digital economy represents an ever-growing part of today's global economy. It is estimated that 60% of global GDP will be digitized by 2022. Across all sectors, UK companies are relying more than ever before on the ability to access data across international borders, to run and improve their internal operations and to connect with their value-chain and better service their customers. By extension, the ability to leverage digital technologies will critically contribute to the UK's economic recovery post-COVID. The UK Data Protection Act (Chapter 5) provides a list of mechanisms that can be used by organizations to comply with the Act's general principles and specific requirements when transferring personal data to third countries. These tools include: adequacy decisions; Standard Contractual Clauses (SCCs); Binding

[13] For more information, see BSA Submission to the ICO Draft AI Auditing Framework Guidance, https://www.bsa.org/policy-filings/uk-bsa-submission-to-the-ico-draft-ai-auditing-framework-guidance

Corporate Rules (BCRs); and other mechanisms. Different organization types and business models require the use of different transfer mechanisms that are not interchangeable. In practice, larger companies will rely on one or more data transfer mechanisms, using the tool most tailored to their business needs and to the specific data transfer(s) at hand. However, many MSMEs and small organizations do not have sufficient legal and financial resources for multiple data transfer tools; they will principally rely only on one mechanism (most likely SCCs, in the absence of a data adequacy agreement). The ability of MSMEs to access global markets and to offer and sell their services and products abroad depends upon cross-border access to the data and cloud-enabled technologies.

- It is important that the UK maintains its international data flows regime so it allows for several options for seamless cross-border data flows across key jurisdictions for the UK economy, and that businesses be able to continue using the full range of existing data transfer mechanisms that support global data flows and are built with strong safeguards, primarily: adequacy decisions; SCCs and BCRs. See response to question 18 for additional input on this point.

Privacy and global interoperability:

The UK will set important global precedents as it reflects on the future of transfer mechanisms post-Brexit. This reflection should consider maximizing interoperability with the existing tools referenced above and encouraging interoperability among data privacy regimes around the world. At a time of rising protectionism across the world, the UK should also continue to promote strong privacy safeguards and international data flows as pillars of the data economy. It should also be a strong voice against localization trends and other restrictions to international data flows.

- As it looks to update its transfer regime, the UK should build on its existing legislative framework by preserving existing tools that have been widely adopted by the business community and by recognizing the power of issuing UK adequacy determinations to countries not yet considered by the EU.
- The UK has an important role to play in driving trust-based governance globally. The UK's involvement in international conversations such as the World Trade Organization Joint Statement Initiative on e-commerce is appropriate as a group of over 80 countries negotiate a new rulebook for e-commerce.

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.

To unlock the value of data across the economy, the UK should establish a policy framework that (1) enhances access to high value government data, (2) makes it easier for organizations to voluntarily share

their own data, and (3) promotes the development and use of privacy-enhancing technologies that enable data collaboration in ways that align with the public's expectation of privacy. Please see our response to Question 6 above for further details and recommendations.

To enable better use of data across Government, we agree with the five areas of work outlined in the Strategy. They are all equally important, but our view is that some of these work areas should be looked at first, as they will provide the basis for the implementation of others.

Capability, leadership and culture should be addressed as a matter of priority.
Building a culture of internal data sharing and accessibility within Government should be the starting point. Government Data is too often held in silos, and the default option is not to share the data across departments or functions. Agencies and departments collect data to serve their own needs and not cross-government uses. This is not just observed in the UK but in most OECD countries.[14] This issue is further exacerbated by a lack of consistent skills, policies, guidance and leadership. With regards to data, Government services are not always rewarded for being innovative and they are faced with a fear of getting it wrong.

To establish a data-sharing culture in the public sector, the UK Government should consider developing a simple risk-based framework based on appropriate compliance and legal controls. Internal data-sharing should be the default option and exemptions should be justified on security, legal or privacy concerns only.

As part of this priority focus on leadership and culture, data skills are required at all levels of Government, including in senior executive teams. Senior leaders do not always have the experience of using data and should receive appropriate training to experiment with data and find new ways to use data to make decisions. Digital skills should be part of the broader response to transforming government's use of data. Advancing short-term and non-traditional training and programs for government workers will help rapid reskilling and upskilling.

A second key underpinning for an effective data-driven government is an effective strategy for Data quality, availability and access.
Poor quality of public sector data is largely due to inconsistencies in data collection practices across public sector agencies and departments. For example, COVID-19 has revealed that some hospitals were still manually inputting COVID-related data. More consistent data collection practices should be put in place for better data quality and productivity benefits in the administration.

[14] A Data-driven Public Sector - OECD Working Paper, https://www.oecd.org/innovation/digital-government/working-paper-a-data-driven-public-sector.htm

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?

Cloud infrastructure security policies should:

- prioritize the assessment, management, and reduction of risk in the systems and services that store, process and transfer data;
- be flexible and allow entities to select the most suitable cloud products for delivering their services in a secure and resilient manner, and thereby promoting a diverse marketplace of solution providers that can compete on the basis of security;
- be adaptable enough to allow all entities to take forward-looking approaches to security by leveraging innovative security approaches to security as technologies change and threats evolve.

One of the key aspects of cloud infrastructure is the shared nature of their security, continuity, and resilience across entities. Instead of a monolithic approach where a single entity takes sole responsibility for establishing and maintaining the entire ICT ecosystem, cloud infrastructure providers and their customers, and any other service providers in the system, take responsibility for different aspects the overall cloud service environment. The overall security of the system cannot be assured without all parties' contributions, and without some coordination of responsibilities among all parties. It is essential that all parties share an understanding of the clear division of responsibility for security between them. This is the shared responsibility model for security of cloud products.

In the context of enterprise Cloud, cloud infrastructure providers operate as seamless extensions of internal IT operations. From a security policy perspective, rather than creating an additional layer of regulation for "hosting/ ICT third party providers," the regulator should instead ensure that enterprise customers, be they critical infrastructures or regular businesses, are managing their third-party relationships pursuant to risk-based policies and procedures that are commensurate with the level of risk posed by the business function that is being outsourced to the said ICT service provider.

To that end, and consistent with international best practices and the shared responsibility model of operations, these enterprises should have the responsibility to ensure that their service agreements with ICT service providers clearly articulate the data governance requirements to which the ICT service provider must comply. Under this agreement the cloud infrastructure provider should provide appropriate evidence and appropriate oversight for enterprises to meet their government responsibilities.

For example, when a financial entity outsources a sector-critical system to an ICT supplier, the financial entity should ensure that the data governance requirements and prudential obligations are accounted for in the service agreement, and in compliance with both the financial entity's and service provider's existing regulatory obligations and operations.

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?

First and foremost, any organization (supply and demand side alike) need to set proper data governance targets, focusing non-exhaustively and based on a risk management approach. The strategies should articulate their data infrastructure needs and consider elements like the assignment of responsibilities with other entities, desired availability of service, the allocation of sufficient resources, the accountability of management, the catalogue of data for the services, the introduction of a risk-based security and resilience approach and the maintenance of an updated register of existing outsourcing and/ or service arrangements. These can then be included in any commercial arrangement with cloud infrastructure providers, setting clear expectations and remedies based in common law.

With regards the contractual arrangement with the technology provider, a harmonized approach to specific clauses included in the contracts helps address existing barriers to the development of cloud adoption and reduce the costs of fragmentation throughout the economy.

- The development of a set of Standard Contractual Clauses for use between enterprise customers and their ICT third party service providers should be done in close cooperation with industry, account for a technology-neutral and principle-based approach and align with existing privacy and other regulatory requirements.
- The use of such clauses should be voluntary, given that cloud deployment use cases are too diverse to make detailed contractual clauses work across all scenarios. It would be difficult to create and single set of Standard Contractual Clauses (or direct regulation) for all outsourcing vendors as there are many different applications that need to be considered, such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), etc. as well as hybrid cloud environments.

Many providers obtain voluntary certifications against internationally recognized standards, such as ISO/IEC 27001 and SOC II, to effectively demonstrate to clients the robustness of security controls and organizational security practices. Such certifications allow for the evaluation of providers according to consensus criteria based on well-established industry best practices. We believe security certifications are most effective when they are voluntary, enabling different providers to compete on the basis of their security practices, and risk based.

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?

As a general rule, the principle of shared responsibility should become the gold standard when considering any future regulatory intervention. This recognizes the different responsibilities in the operation of cloud data infrastructure, and holds entities responsible for the aspects of the environment over which they can be held accountable.

- Regulatory obligations should therefore treat cloud computing in a similar way as other types of outsourcing, recognizing that both the cloud provider and its customer share security responsibilities and that therefore moving data & computing platforms to the cloud do not transfer ultimate responsibility for data, device, user and network security to the service provider.

The Government has a role to play in many aspects of ensuring security, continuity and resilience of service for cloud infrastructure providers. These include:

- contributing information to help inform the risk assessments of enterprises,
- helping enterprises understand the importance or a whole-of-lifecycle approach to IT security and technology supply chain security, and
- providing training on how to conduct risk assessments of supply chains. They can provide the community with information on appropriate widely accepted, risk-based security standards.

Governments should be careful about mandating controls that, whilst well intentioned, can reduce the security and resilience of cloud infrastructure. For example, a policy that mandates registering the exact location of data centres reduces the physical security of these assets, and mandating data localization can reduce the resilience of the cloud product or service.

BSA would welcome further discussion with the Government of the UK on ways they can help in this respect.

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.

Given the diverse range of use cases, it would be impractical to limit the identification of risk factors through a one-size-fits-all approach. Determining whether any particular factor is "important" or "critical" can only be achieved by understanding the particular business need and security requirements, and following a proper context-specific risk assessment.

In most cases, security and resilience demands a holistic approach in which risk factors from all relevant hazards are considered, prioritized, and mitigated comprehensively. In this context, it is important to note that government policies can create additional risk when they constrain the ability of providers to adopt diverse strategies for risk mitigation; in particular, policies requiring localization of data or restricting its transfer adopted recently in some countries constrain the ability of providers to establish redundant data storage and processing, thus undermining resilience. This ability to respond in a risk management approach can also be undermined when governments mandate specific controls, no matter how well intentioned.

For example, government cloud infrastructure policies should help organisations design their cloud environments by taking a risk management approach to availability to reduce costs by better tailoring their cloud product choices to business processes. As a result of this analysis a business may choose to use a product with lower availability, and subsequently lower cost, for less critical processes, and cloud products with higher availability for critical processes and data.

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

As the world responds to the climate crisis, and governments make commitments to be net zero or net negative on emissions, the use of data will play an ever increasing role in helping shape public policy solutions that drive sustainable and inclusive economic growth whilst helping reduce carbon emissions. In this situation the National Data Strategy should be seen as part of the government's wider sustainability agenda.

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?

As indicated above (see question 10), a robust international transfer regime should be a cornerstone of today's trust-based digital economy. The UK Privacy Act provides solid foundations for an international transfers regime as it recognizes the importance of the free flow of personal data with strong safeguards, and provides tools for organizations to legally transfer personal data abroad.

- We urge the UK Government to prioritize the interoperability of the UK Privacy Act transfer mechanisms with other mechanisms used in leading global privacy frameworks. In other words, it is important that the UK recognize the use of existing global mechanisms that meet the UK's standards rather than requiring the use of new UK-only mechanisms.

Beyond the data transfer mechanisms recognized by the UK Privacy Act, trade commitments and disciplines can play an important role in diversifying and solidifying mechanisms that underpin cross-border data flows. The UK stands to benefit from an ambitious digital trade agenda that preserves the ability of UK companies to transfer data across borders, strictly limits data localization requirements, and precludes the forced transfer of, or access to, software source code or algorithms. Working towards accession to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) will bring benefits of such provisions not only to UK citizens, but also to service providers and manufacturers that rely on data analysis, AI, and cloud computing services to grow. The financial sector for instance, consistently uses AI's assistive traits to enhance customer experience and protect assets. Banks leverage AI-based tools to create and deliver more efficient processes and services by monitoring global activity and identifying malicious actors. AI also helps predict credit risk, monitor for online fraud, and forecast economic occurrences that can affect consumer decisions and business outcomes. Likewise, the transportation sector – from jet engine R&D to transportation services – depends heavily on software and AI. This includes the deployment of knowledge-based design software at Rolls Royce PLC, and the deployment of AI-enhanced enterprise software solutions at Transport for London, a local-government organization responsible for most aspects of London's transport system.

- The UK should continue to work towards modern digital trade provisions in its bilateral and plurilateral agreements as a way to support its digital economy. This will also serve as a critical example for other countries hoping to develop their own digital trade rules and set an important precedent for future trade negotiations around the world. The UK should strive to play a thought-leadership role as the global conversation on multilateral digital trade rules and convergence of privacy regimes continues.

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?

As noted above, the UK should continue to ensure a robust international transfer regime that recognizes multiple stable and trusted mechanisms for companies to transfer data across international borders. While adequacy determinations can be one important mechanism for supporting international transfers, we want to emphasize the need to ensure other mechanisms continue to support international transfers, including SCCs and BCRs. The importance of having several different mechanisms for companies to use to transfer data is only heightened now, after a recent decision from the European Court of Justice[15] led to the invalidation of the EU-US Privacy Shield and created new obligations for companies transferring data pursuant to SCCs.

To ensure the UK's international transfer regime is interoperable with existing global data transfer mechanisms, we recommend the UK approach adequacy determinations with a presumption that the UK deems adequate any country that has received an adequacy determination from the EU. This approach would not only foster interoperability between the two regimes, but also enable the UK to prioritize adequacy determinations for countries that have not yet been examined by the EU for potential adequacy.[16] Aside from EU countries which would fall under the UK adequacy decision for the EU, the countries currently without an EU adequacy determination include top UK trading partners such as the US (15.5% of UK exports), Hong Kong, Japan and Singapore which represent between 1.5% and 2% of UK exports. Within this list, only Japan is currently recognized adequate by the EU.

- By adopting an independent international transfers regime, the UK could seize the opportunity to strengthen transfers to these key trading partners. The UK's adequacy determinations for these countries would also set an important global example for other countries addressing similar issues under their own data protection frameworks.

Moreover, as the UK takes on the role of making adequacy determinations, it is important to bear in mind that adequacy is increasingly conceived as a living mechanism that can be adapted to evolving business and legal realities through periodic reviews, which can help to ensure the durability of those determinations.

- Expanding the list of countries recognized as adequate would provide UK organizations with a valuable alternative mechanism for transfers to these countries. In order to determine priority countries for possible adequacy, the relevance for business and commitment to similar values should be guiding criteria of the UK approach.

For further information, please contact:
Isabelle Roccia
isabeller@bsa.org

[15] ECJ press release on Schrems vs. Facebook : https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

[16] The European Commission has so far recognized Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay as adequate. Negotiations are underway with South Korea and the United Kingdom.