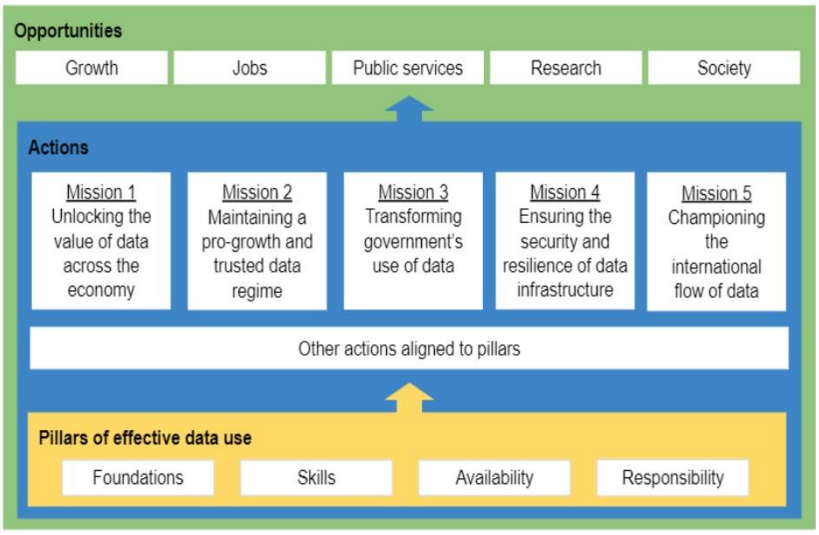
IRSG RESPONSE – UK NATIONAL DATA STRATEGY

CONSULTATION QUESTIONS & ANSWERS



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 IRSG support the missions and pillars of the National Data Strategy, and welcomes the opportunity to respond to this consultation. According to a recent House of Lords report[1], Financial services, professional services and business services form the largest part of the UK economy, and data drives these sectors. We would therefore like to highlight some priority issues.

Data quality and data accessibility are key.

In regards **data quality**, we still have a lot of incomplete, non-existent or biased data in the UK both in the public and private sector. This is a particular issue for diversity and inclusion. By way of example, a 2019 study conducted by the Massachusetts Institute of Technology found that none of the facial recognition tools from Microsoft, Amazon and IBM were 100% accurate when it came to recognising men and women with dark skin[2]. The is widespread concern that many of these datasets that such tools are trained on are not sufficiently diverse to enable the algorithms to learn to correctly identify non-white faces. Therefore, the impact of such datasets on AI and other data-driven innovations is significant , and biased input will yield biased output. The sector also feels that UK competitiveness is affected by the lack of data on professional services and business services, e.g. from the ONS. This is in comparison to the significant amount of data on goods, manufacturing etc.

[1] https://publications.parliament.uk/pa/ld5801/ldselect/ldeucom/143/143.pdf
[2] https://www.bbc.co.uk/news/technology-47117299

We cannot solve for tomorrow's challenges without collating the relevant and applicable data for analysis, and incomplete data gives us only half of the story. The US and China who lead in innovation know this, and collect an extraordinary amount of data from as many sources as possible. In 2012, only 0.5% of all data was analysed[3]. Now, the big data analytics market is set to reach $103 billion by 2023, and it is estimated that every person has generated 1.7 megabytes of data per second in 2020[4]. In many ways, it is a virtual race to acquire data, limited only by technical and legal restrictions where applicable.

For **data accessibility**, we need to ensure we can use data from both the public and private sector to support innovation and AI. Ensuring that the UK does not fall below 3rd place for innovation, after the US and China. To do so, we need to break down data silos to enable responsible access to and use of data to support innovation and growth and to enable risk management to be more effective.

The IRSG supports **interoperability** rather than creating more data standards which are often national, and sector- or technology-specific. These can therefore create more barriers to data sharing. In reality, these standards need to exist at an international level, with an emphasis on agreed data taxonomies which can then be fed into. The issue with standards is that they can quickly become obsolete, so we would suggest focusing on agreed taxonomies designed to support interoperability and data sharing, so that data held in whatever standard, is held in a manner which will allow it fit into the taxonomy and be shared. In addition, **data needs to be smart.** Consumers should retain control of their own data that they generate, and be able to safely and securely transfer this data to trustworthy third-party services who can use this data to provide innovative services for consumers.

Furthermore, the IRSG would also like to highlight the potential value of '**Digital IDs'** or 'Digital Passports' in unlocking access to banking, government benefits, education, and many other critical services for individuals. It is important that these are taken into consideration in the development of this Strategy, with any initiative following principles of privacy, transparency and good governance.

Lastly, we would like to highlight the dependence on **third-country technology** on which our communications and businesses are wholly reliant. As has been demonstrated during COVID-19, the likes of Microsoft Teams, Google Meet or Zoom, to name but a few, have been critical to the continuity of education, business, government and personal communications. We should question whether we are content to build our future data strategy on the borrowed bricks of third country technology, and whether we have considered the concentration risk that this can give rise to. This is further explored later in our response.

Q4. We welcome any comments about the potential impact of the proposals outlined in this consultation on the UK across all areas, and any steps the government should take to ensure that they take account of regional inequalities and support the whole of the UK?

The IRSG welcomes the ambition in the Strategy, but would like to highlight that the Strategy is wholly reliant on the physical data infrastructure, by which we mean the infrastructure which enables everyone in the UK to have high speed and quality access to the internet.

As more people work remotely and need a digital connection due to COVID-19, our current infrastructure has proven inadequate. The future of work post COVID-19 means increased remote working and a need for robust and equality of digital connections. However, it remains the case that too many parts of the UK, both urban and countryside, continue to have poor internet access. We urge HMG to do as much as they can to meet their pledge to have next-generation fibre broadband across the UK by 2025.

[3] https://www.theguardian.com/news/datablog/2012/dec/19/big-data-study-digital-universe-global-volume#:~:text=The%20global%20data%20supply%20reached,to%20the%20Digital%20Universe%20Study.&text=In%202012%20less%20than%20a,despite%2035%25%20requiring%20such%20measures.
[4] https://techjury.net/blog/big-data-statistics/#gref

Digital infrastructure, both internet access and the technology on which we operate, needs to be able to safely support national data ambitions both for individuals (especially education) and business (especially SMEs) access to data. This can enable better financial inclusion and access for vulnerable consumers.

MISSION ONE: UNLOCKING THE VALUE OF DATA ACROSS THE ECONOMY

Q5. Which sectors have the most to gain from better data availability? Please select all relevant options listed below, which are drawn from the Standardised Industry Classification (SIC) codes.

- Accommodation and Food Service Activities
- Administrative and Support Service Activities
- Agriculture, Forestry and Fishing
- Arts, Entertainment and Recreation
- Central/Local Government inc. Defence
- Charity or Non Profit
- Construction
- Education
- Electricity, Gas, Steam and Air Conditioning Supply
- Financial and Insurance Activities
- Human Health and Social Work Activities
- Information and Communication
- Manufacturing
- Mining and Quarrying
- Transportation and Storage
- Water Supply; Sewerage, Waste Management and Remediation Activities
- Wholesale and Retail Trade; Repair Of Motor Vehicles and Motorcycles
- Professional, Scientific and Technical Activities
- Real Estate Activities
- Other **(All of the Above)**

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

We believe the growth of data-driven service offerings, across multiple sectors, will be strengthened by political and regulatory support. IRSG members have experienced Open Banking, and the benefits it has brought in terms of greater customer choice. However, we support other sectors following suit in terms of sharing their data with other each other, to ensure all sectors can benefit from the Strategy. To this end, we support the UK Government's Smart Data initiative, and look forward to further data sharing initiatives, beyond the Financial Services sector.

HMG should also seek to improve the quality of government held data to ensure both SMEs and large organisations have access to data to innovate and grow. Notably, this data could assist with verifying identity as part of risk assessments and authentication processes in the fight against financial crime. However, data sharing frameworks need to strike the right balance between mandatory and voluntary data sharing and certain data may not be shared due to its sensitivity. Data sharing must also protect legitimate commercial and IP interests of the sharing entity. It is paramount to ensure new entrants are subject to the same standards as traditional incumbents.

In addition, HMG should also convene different sectors together to facilitate the development of data sharing opportunities, including at the international level, which is a better place for taxonomy standards, as mentioned above.

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

While the needs of different sectors are different, IRSG Members have highlighted that it is not unreasonable to assume that UK competitiveness is affected to some extent by the lack of data. This has become clear throughout the Brexit process. Due to poor depth and quality, it was initially difficult to find reliable data on existing data flows with the EU, existing trade with the EU etc.

In many instances, the data is simply not available. There is a significant amount of data on goods, manufacturing etc, but not so much data on trade in services. HMG could use this convening role to enable the creation of new data sets to support business to identify opportunities and to innovate and grow.

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

For the IRSG, HMG's role is to set the policy and agenda, and it is the role of business to implement according to sectoral needs. As mentioned, government should be a convener to identify where there are challenges and blocks to accessing, using and sharing data and to legislate if needed to overcome those challenges and blocks.

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?

Above all, the IRSG would like for the UK's data protection framework to continue with a risk based and outcome focussed approach to regulation and enforcement, focussing on the practical impact for individuals. The ICO should continue with consultation, transparency, sandboxes, guidance, and openness to explore how existing principles apply to future innovation. By way of example, the IRSG welcomed the ICO's COVID-19 response which was pragmatic and helpful as opposed to simply repeating legal obligations.

There should also be continued engagement across UK regulators to ensure consistency, e.g. across competition, consumer legislation, AML etc to ensure a joined-up UK approach, where data protection obligations support and clarify rather than conflict with other regulatory obligations. In addition, the UK should continue to engage with the EU and international regulators and legislators to continue to build bridges and interoperability, and to avoid fragmentation of data protection and data localisation.

Whilst the IRSG supports the need to maintain high data protection standards we are concerned with the evolution of representative actions in the English courts. While conflicting with past decisions and

subject to appeal, the recent case *Lloyd v Google*[5] set the legal bar for compensation at a mere "loss of control of personal data" irrespective of any actual harm caused to affected individuals or the interest of those individuals in pursuing claims. Coupled with the rise of litigation funding, there is a significant risk of vexatious and potentially ruinous claims for compensation, whether those claims are ultimately successful or not, undermining the objectives of the UK National Data Strategy.

There is ample evidence from jurisdictions which have had class action claims for several decades that the actual benefit for consumers is unproven. In the US, the uptake rate on settlements (the percentage of the class that actually takes the time to fill out a claim form to partake in the settlement) is now tracking below 5%, and can be as low as 2%, so very few purported victims of the complained harm actually ever receive compensation. In contrast claimant lawyers and their funders have done extremely well from class action often securing 25% plus of the settlement awarded.

In the UK where there is and will continue to be extensive regulation of the processing of personal data including the potential for revenue-based fines under the UK GDPR, and so there is no need for an additional deterrent of representative actions. Organisations already have a very strong regulatory incentive to ensure compliance with data protection law – and if a large group of affected individuals wish to pursue claims there is the separate "group litigation" regime already available under the civil procedure rules.

HMG should revisit whether representative actions for data protection claims are in the public interest given their limited benefit for consumers and the significant disincentive they create to invest in the UK and innovate in the digital economy.

The IRSG supports utilising technology to ensure the data protection framework in the UK stays fit for purpose. For example, greater government support for privacy enhancing technologies and anonymisation and pseudonymisation techniques which facilitate a better utilisation and analysis of personal data whilst retaining privacy.

In sum, data is an enabler for financial services, professional and business services. Our sector needs privacy legislation and civil court procedural rules to provide strong standards but with a balanced approach. The UK can play a national and international thought leadership role in the evolving role of privacy to safeguard data and support innovation and growth initiatives.

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.

Quality, availability and access to data is indeed a priority. The quality of government data would improve if data is shared between government departments to ensure consistency and address out of date, incorrect and incomplete data. Likewise, **ethics and public trust** are critical to enable the use and

[5] Lloyd v Google LLC [2019] EWCA Civ 1599

access to data. We support continued high standards of data protection, as well as education and awareness of how data is used and how individuals can better protect their data.

As mentioned earlier, the IRSG would also like to highlight the potential value of an interoperable digital ID system as one of the central building blocks of a connected, data-driven digital economy. We believe that a digital ID can bring business and societal benefits including fraud prevention, financial inclusion, and improved security for businesses.

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 IRSG supports the UK's stance on discouraging data localisation, but calls on HMG to consider the UK's exposure to concentration risk regarding Cloud, technology and infrastructure providers. At present, our schools and businesses are almost exclusively reliant on technology from a handful of third-country providers, and are increasingly dependent on them to operate, store data and communicate. When reliance is concentrated on so few providers and specific jurisdictions, it lends itself to becoming a significant cyber risk as well. The EU's Digital Operational Resilience in the Financial Sector Act (DORA) is one approach to address these challenges, but it has unhelpful elements of data localisation. The general IRSG position is that this is not an attractive option.

Instead, the UK can demonstrate its capability, leadership and culture in data through international forums and in the Strategy by ensuring fair and transparent data protections which can support data use and innovation. Fragmented national regulatory requirements for Cloud increase the cost and complexity of implementation and the risk for Cloud governance. Internationally, we have observed that the trend has been to treat Cloud as a subset of outsourced service provision and apply legacy outsourcing concepts to Cloud services, which does not address emerging risks.

There is an opportunity for a fair and balanced approach going forward which sits between the rights-focused GDPR, and the fragmented legislative approach in the US. This would require developing a more mature accountability framework, and needs to be done at a government, not business-to-business contractual, level.

By rejecting data localisation, the UK should focus on being a convenor of similarly minded jurisdictions that have significant market and regulatory power, creating opportunities to level up standards in a helpful way. Should HMG choose to place requirements on virtual or physical infrastructure providers, any approach should be risk-based and proportionate, support international cooperation and avoid national variations in rules that undermine the efficiency gains of Cloud.

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?

Data infrastructure services tend to provide the tools to the user, so they are responsible for their own security and use of the services, e.g. for configuration etc. Firms that use the service providers perform comprehensive due diligence in accordance with policies and procedures, and in line with regulatory requirements, before onboarding and throughout the relationship. The service provider therefore has a level of responsibility, but so do regulated entities that use the infrastructure. Nevertheless, these can be difficult to understand and implement, especially for SME's who may lack highly complex and developed technology skills. A basic level of assurance is needed, e.g. the default is private, not public.

Cyber threat actors are increasingly focussed on finding "gaps" in security to exploit. As noted above, there is, in reality, very limited choice when it comes to data infrastructure services and providers. This creates what could be seen as a very significant risk of concentration of providers, and limited choice for individuals and businesses.

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 previously mentioned, the IRSG believe that there is an opportunity for the UK to be an international thought leader, facilitator and convener of similarly minded countries, to agree a common and level playing field and platform for mutual recognition, interoperability etc. The UK should leverage soft law and influence to ensure others adhere to similar standards. Two-thirds of the world now has privacy laws, but we also have multiple and differing standards rather than a more level playing field.

In addition, regulatory cooperation should be promoted to ensure greater consistency. In financial services, regulators can cooperate to implement global interoperability of standards. Memoranda of understanding between government and regulators are helpful regarding data sharing, but we also need something which works for and addresses business data sharing. Furthermore, there is a need to ensure the whole ecosystem is captured as firms rely on outsourced suppliers, experts, and infrastructure to operate. These all need to be within scope, not just "regulated" entities. For example, financial crime and cybersecurity are global issues with multi-tiered participants supporting the financial and broader business ecosystem.

Lastly, it is also important to understand cultural differences vis-à-vis privacy and data sharing, in order to best improve international transfer mechanisms.We urge HMG to use the upcoming UK Presidency of the G7, and role as Chair of the Digital Nations forum, in 2021, to take a lead internationally and suggest a strong digital agenda.

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 the UK's biggest exports are financial, professional and business services, the IRSG suggests that HMG should focus on those countries which are our main trading partners. This is particularly important for our sector, which requires data flows to customers and service centres. This means, as a first step, ensuring unhindered data flows with the US, EU, Singapore, Hong Kong and India. The IRSG would also like HMG to reach out to countries who have established laws and regulators, and regimes that have credible and substantially similar to our own, e.g. Australia, Canada, New Zealand and possibly Brazil. Switzerland is also an important market for the UK and financial services.

We also suggest that multilateral approaches, to which countries can adhere to, should be examined and prioritised. This may be of particular value with Asian jurisdictions. HMG should look to the APEC privacy model, CBPR, and foster something better or complementary. For Australia, sector-focused adequacy may also be possible.

In any case, adequacy should be subject to regular review and validation, e.g. privacy regulators now publish annual reports. Breaches and regulatory action are more transparent as a result to businesses and the public. There is more to adequacy then legal equivalence; regulatory cooperation and accountability plays an important role. In addition to a country level adequacy assessment, the UK

should promote privacy regulator improved engagement to ensure more consistency around applying privacy rules and sanctions.

IRSG DATA PROTECTION WORKSTREAM – MEMBERSHIP

The workstream is chaired by Vivienne Artz (Refinitiv) and includes representatives from financial services firms, trade associations, the legal profession and data providers.

The workstream includes representatives from:

- ABI
- AFME
- AIMA
- Bank of America
- BNY Mellon
- CBI
- Citi
- Clifford Chance
- Credit Suisse
- DLA Piper
- Fidelity
- FLA
- Freshfields
- HSBC
- IA
- Invesco
- IBM
- JP Morgan
- Lloyds Banking Group
- London Stock Exchange Group
- Marsh Ltd.
- Morgan Stanley
- Nasdaq
- PIMFA
- Refinitiv
- Standard Chartered
- techUK
- UK Finance