BCS - The Chartered Institute for IT Response to National Data Strategy November 27, 2020

RESPONDENT DETAILS	
Name	Dr Bill Mitchell OBE
Position	Director of Policy
Organisation	BCS – The Chartered Institute for IT
Sector	Chartered Professional Body

BCS
The Chartered Institute for IT
3 Newbridge House,
Newbridge Square,
Swindon SN1 1BY

BCS is a registered charity: No 292786

Table of Contents

Executive Summary

As explained by the Rt Hon. Oliver Dowden CBE MP the National Data Strategy[1] is intended to fulfil the "*government's wider ambition for a thriving, fast-growing digital sector in the UK, underpinned by public trust*". While we broadly agree that the Strategy will support this ambition, in our view the central pillar of 'Responsible Data' in the Strategy conflates three vitally important areas that should be separated out into pillars in their own right to ensure they are given suitable prominence when the strategy is executed in practice. The pillar of 'Responsible Data' should be separated out into these three distinct pillars:

- Building public trust in data driven services,
- Ensuring data is always used responsibly, and
- Developing a sufficient supply of competent, ethical and accountable computing[2] professionals across all sectors of the economy.

Figure 1 illustrates how the original 'Responsible Data' pillar can be split into these three new pillars (shown in brown), which then wrap around the other three pillars (in blue) from the Strategy.

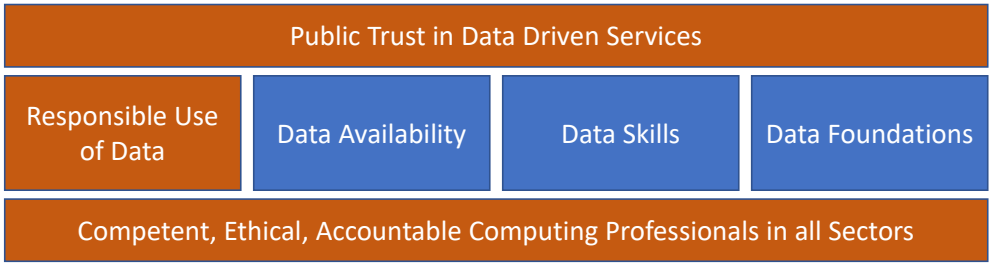

Figure 1: National Data Strategy Pillars with three key areas separated out as pillars in their own right

Seen in this light the following recommendations support delivery of the National Data Strategy as rapidly as possible and optimise value for money. Government should:

Demand that professionals who develop computer software used to deliver public services, or that is used to inform public policy, such as for example developing computer models of climate change, or who manage the adoption of such software by the public sector, must be Chartered by a relevant professional body.
Set the expectation that all computing undergraduates are assessed on their professional competency against widely recognised standards, as well as on their academic ability.
Galvanise the development of a broad range of professional computing qualifications at all levels that supports progression to Chartered status.
Work with all professional bodies (not just computing) to support incorporating relevant digital and data competencies within their professional recognition (e.g. aspects of Artificial Intelligence and Machine Learning are becoming important to data science roles in accountancy).

[1] https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy

[2] we take computing to be a catch all term covering computer science, digital technologies, data science, artificial intelligence, machine learning and cyber security

Government is already doing much to support professionalism across computing related professions. Government has set out in the National Data Strategy, in its AI sector deal, the UK National Digital Skills Strategy, the Cyber Security Skills Strategy and before that in its Industrial Strategy the vital importance of highly skilled professionals in computer science, digital technologies, data science, artificial intelligence, and cyber security.

The National Data Strategy recognises the work being done by the Royal Statistical Society alongside BCS, the Operational Research Society, the Royal Academy of Engineering, the National Physical Laboratory, the Royal Society and the Institute of Mathematics and its Applications working to develop data science as a profession[3]. BCS, The Society of Research Software Engineering and the Software Sustainability Institute are also working together to promote professional standards for coding used in scientific research. This is particularly relevant in the wake of high profile challenges[4] to scientific modelling used in COVID-19 policy.

Government is funding a consortium led by the IET in partnership with BCS and fourteen other professional organisations to set up the UK Cyber Security Council, which will establish Cyber Security as a profession governed by a Royal Charter. The NHS is supporting the Federation for Informatics Professionals in health and care (FedIP), created in 2016 to professionalise the informatics community in the UK in Health and Social Care.

These are all important steps in developing professionalism in line with the pillars set out by the National Data Strategy, but are no longer sufficient in the world we now live in outside of the EU and post COVID-19. Recent YouGov surveys[5] of the UK public commissioned by BCS show that

- Over half (53%) of UK adults have **no faith** in any organisation to use algorithms when making judgements about them, in issues ranging from education to welfare decisions.
- 63% of UK adults **disagree** with the statement "*Students graduating with a computer science university degree are qualified to write software that makes life decisions about people*"
- 62% of UK adults believe someone who for a living develops computer software that can significantly affect people's lives should be qualified as a government-approved **Chartered professional**

Further details of the surveys are given in our full answer to question 1 of the consultation in the following sections.

Chartered status of a computing practitioner gives the public confidence that the practitioner is competent, ethical and accountable (in this case accountable to their professional body). Professional bodies already exist and have an effective infrastructure for

[3] https://royalsociety.org/-/media/policy/projects/dynamics-of-data-science/dynamics-of-data-science-skills-report.pdf
[4] https://www.nature.com/articles/d41586-020-01685-y
[5] https://www.bcs.org/more/about-us/press-office/press-releases/the-public-dont-trust-computer-algorithms-to-make-decisions-about-them-survey-finds/

managing Chartership, which is by definition backed by a Royal Charter that ensures it remains independent, objective and must work for the benefit of the public. Demanding computing professionals in responsible roles are Chartered therefore presents a readymade and cost effective solution to the issue of rebuilding public trust, which is a solution the public say they want, and will significantly support delivery of the National Data Strategy pillars.

Detailed responses to consultation questions

The rest of this document gives the BCS responses to questions in the consultation.

Question 1

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.

Please see the Executive Summary for the main recommendations that form our response to this question. The remainder of the section gives the background context that explains our reasoning for those recommendations, which follows on from a presentation BCS gave at the November 2020 roundtable hosted by Caroline Dinenage Minister of State for Digital and Culture at DCMS.

Why we recommend separating out the Responsible Data pillar

The National Data Strategy states:

- "The strategy is a central part of the government's wider ambition for a thriving, fast-growing digital sector in the UK, **underpinned by public trust**."
- "Used badly, data could harm people or communities, or have its overwhelming benefits **overshadowed by public mistrust**."

Public trust is founded on the knowledge computing practitioners are

- ✓ Competent
- ✓ Ethical
- ✓ Accountable

Unfortunately, public trust has been seriously eroded by events over the last six months, as we summarise in the next section.

High profile examples that undermined public trust in use of computing for public services since May 2020

Between May and November of 2020 there has been a constant series of high profile incidents that have significantly eroded public trust in the use of computing in public services. Here we list those examples and then summarise the findings from two national surveys BCS commissioned YouGov to conduct that show how badly public trust has been eroded.

MAY: In May there were a series of high profile articles in the national press, such as for example in the Telegraph[6], that asserted computer code developed by Professor Niel Ferguson to model the spread of COVID-19, and which was key to government decisions about imposing national lockdown, was highly flawed and implied it was not fit for purpose.


Coding that led to lockdown was 'totally unreliable' and a 'buggy mess', say experts

The code, written by Professor Neil Ferguson and his team at Imperial College London, was impossible to read, scientists claim

By Hannah Boland and Ellie Zolfagharifard

16 May 2020 • 1:32pm

The Telegraph

Neil Ferguson was one of the key architects behind the Imperial model

Figure 2: example of highly critical national press item on computer code underpinning epidemiological model

Since then Professor Ferguson's epidemiological computer code has been shown to be fit for purpose, for example in articles[7] in the scientific journal Nature. The general public however do not read Nature and are mostly only aware of articles such as those in the Telegraph that were highly critical.

What became apparent during this episode is that the scientific community[8] has not in general adopted software development standards that would ensure their computer code is easy to reproduce and be understood by the wider scientific community. This has become a major issue across the global scientific community[9]. Such standards do exist, such as those developed by the Software Sustainability Institute (SSI). BCS is now collaborating with the Society of Software Research Engineers and SSI on increasing the adoption of these software development standards across all of science.

MAY: The NHS COVID-19 contact tracing app was meant to launch in May, but was pushed back to September because of a series of technical difficulties and issues with ensuring ethical data gathering and processing[10]. Additionally, it didn't work as Public Health England

[6] https://www.telegraph.co.uk/technology/2020/05/16/coding-led-lockdown-totally-unreliable-buggy-mess-say-experts/
[7] Nature reproducibility: Critiqued coronavirus simulation gets thumbs up from code-checking efforts
[8] https://www.bcs.org/media/5780/professionalising-software-development.pdf
[9] https://www.bbc.co.uk/news/science-environment-47267081
[10] https://www.bbc.co.uk/news/technology-53114251

wanted because of Google and Apple privacy concerns that meant the technology was prevented from collecting data as intended.

Figure 3: public trust was eroded by ongoing difficulties with launch of the contact tracing app

BCS prior to the launch of the app had laid out the ethical practicalities that would need to be addressed in a policy paper[11].

AUGUST: In August Ofqual used an algorithm to estimate GCSE and A-level grades that resulted in widespread public mistrust in algorithms making high stakes decisions about people[12], which resulted in the Secretary of State for Education having to make a public apology.

Figure 4: BBC News item of public apology from the Secretary of State for Education about 'Ofqual algorithm'

BCS published a policy paper[13] after the incident explaining why data driven algorithm design is challenging and requires interdisciplinary teams of professionals working collaboratively and to the right professional standards in order to make algorithms work as intended.

OCTOBER: In October Public Health England lost 16,000 COVID-19 test results due to human error when importing data from a CSV[14] file into an Excel spreadsheet.

[11] https://www.bcs.org/media/5689/contact-tracing-report.pdf
[12] https://www.bbc.co.uk/news/uk-53815089
[13] https://www.bcs.org/media/6135/algorithms-report-2020.pdf
[14] CSV: comma separated values, which is a standard format used for sharing tables of data between different proprietary spreadsheet and database applications.

Figure 5: https://www.bbc.co.uk/news/technology-54423988

Members of the public understandably questioned the apparent inability of Public Health England to automate such a routine but vital part of their data handling, which affected the public's perception of the digital competency of PHE.

NOVEMBER: In November the Public Accounts Committee published a highly critical report[15] on progress with NHS Digital Transformation. The committee commented that:

- The Department and National Health Service have a poor track record for transforming NHS IT and have made insufficient progress against national ambitions
- The Department's previous attempt to reform how the NHS uses IT, running between 2002 and 2011, was both expensive and largely unsuccessful
- The use of digital services within the health and social care system has increased during the COVID-19 pandemic—including providing more services remotely—showing the substantial potential for organisations to use digital services more and adapt quickly

Such a report from one of the most respected parliamentary select committees significantly added to the general sense that there is a lack of competence around digital programmes within the public sector. The report follows on from a NAO report[16] with similar conclusions.

Figure 6: Front page of NAO report on NHS Digital Transformation

NOVEMBER: Also in November more highly critical national media stories appeared concerning IT problems with the test and trace system, such as for example in the Daily Mail on November 12th shown in the following figure.

[15] https://publications.parliament.uk/pa/cm5801/cmselect/cmpubacc/680/68002.htm
[16] https://www.nao.org.uk/wp-content/uploads/2019/05/Digital-transformation-in-the-NHS-Summary.pdf


Daily Mail

Bungling Test and Trace scheme was hit by 'huge' IT problems last month 'that led to delays in squashing outbreaks in care homes' - as official data suggests system is finally getting better

Figure 7: Daily Mail story on IT problems with test and trace system

YouGov national surveys on public trust in September and October

BCS became seriously alarmed by the above incidents as it became clear the public were beginning to distrust the very notion of using algorithms to deliver public services. We commissioned YouGov to conduct two national surveys of representative samples of the UK adult population across all devolved nations to find out how badly public trust had been eroded.

The headline results from those surveys were:

- Over half (53%) of UK adults have **no faith** in any organisation to use algorithms when making judgements about them[17], in issues ranging from education to welfare decisions.
- 63% of UK adults **disagree** with the statement "*Students graduating with a computer science university degree are qualified to write software that makes life decisions about people*"
- 62% of UK adults believe someone who for a living develops computer software that can significantly affect people's lives should be qualified as a government-approved **Chartered professional**

The following lists the detailed questions and responses from those surveys.

Question: Which, if any, of the following organisations do you trust to use algorithms to make decisions about you personally:

Base: All UK adults	2076
The Government	10%
Social media companies (e.g. Facebook, Instagram etc.)	8%
'Big Tech' companies (e.g. Apple, Google etc.)	11%
Financial services (e.g. banks, insurance companies etc.)	16%
Health and social care (e.g. the NHS, private health care, the council etc.)	17%
Armed Forces	7%

[17] https://www.bcs.org/more/about-us/press-office/press-releases/the-public-dont-trust-computer-algorithms-to-make-decisions-about-them-survey-finds/

The education sector	7%
The police	11%
Social Services	7%
National Security and Intelligence services	12%
Housing associations	6%
Other	1%
Don't know	16%
I do not trust any organisations to use algorithms to make decisions about me	**53%**

Question: Who, if anyone, do you think should be responsible for ensuring that digital technology is used to solve ethical issues?

Base: All UK adults	2063
Politicians	22%
Universities	18%
Technology companies (e.g. Apple, Google etc.)	23%
An independent regulating body	**59%**
The individual computer programmer	13%
Other	3%
Don't know	13%
I do not think anyone should have responsibility for this	14%

Question: To what extent do you agree or disagree with the following statement?

"Students graduating with a computer science university degree are qualified to write software that makes life decisions about people"

Base: All UK adults	2063
Strongly agree	2%
Tend to agree	16%
Tend to disagree	32%
Strongly disagree	31%
Don't know	19%
Net: Agree	**18%**
Net: Disagree	**63%**

Question: To what extent do you agree or disagree with the following statement:

"Someone who develops computer software for a living that can significantly affect people's lives, should be qualified as a government-approved Chartered professional"

Base: All UK adults	2063
Strongly agree	22%
Tend to agree	40%
Tend to disagree	11%
Strongly disagree	6%
Don't know	21%
Net: Agree	**62%**
Net: Disagree	17%

Question 2

Q2. We are interested in examples of how data was or should have been used to deliver public benefits during the coronavirus (COVID-19) crisis, 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.

The digital divide is a critical area where more data is needed to inform urgent action to ensure we see real 'levelling up'. This is particularly critical in education. In April we conducted in-depth interviews with a representative sample of schools in the most disadvantaged areas, covering

- Cumbria

- Northumberland and Tyneside
- Midlands
- London

Between them the schools we talked to have an estimated population of 2000+ students, which means this snapshot is suitably valid.

What it's like for disadvantaged children in those areas:

- Many live in homes without access to fixed line broadband
- Some parents are using 4g data plans as their sole access to internet, when that runs out children don't have access until their monthly plan is renewed
- Not all families have access to a PC or laptop
- Many children sole tech device is a 'hand me down' phone and the screens on them are often too small for doing any worthwhile learning
- Many children have to share phones/devices as families don't have enough to go round
- Where children have some access to better devices it's often a games console or tablet they have to share with siblings.

As an example, one school in Midlands with more than 50% FSM students reported that:

- Only 40% of parents said their children accessed the digital tools that the school provides

Government is now issuing laptops and 4G wireless routers into schools to help reduce the digital divide. It should also gather widespread and longitudinal data on this issue to ensure interventions are having the desired effect. Data on the effective use of digital technology in teaching is also required to advance the ed-tech sector.

Question 3

Q3. If applicable, please provide any comments about the potential impact the proposals outlined in this consultation may have on individuals with a protected characteristic under the Equality Act 2010?

Some individuals with protected characteristics will be less likely to declare culturally sensitive personal data to Government, companies or the public sector, and as a result may face significant barriers to engaging with data driven public services. This may be the case for individuals from ethnic minority groups, individuals of faith, LGBT people, or those with disabilities due to a cultural lack of trust in authority, corporations or data governance structures, which exacerbates as their trust and confidence erodes through negative experiential evidence and media portrayals. Already internet scraping across different social media platforms can aggregate snippets of information that may collectively infer intimate details about someone, leading to the potential for online harassment, intimidation or discrimination. Peers or colleagues may inadvertently post information on social media that can facilitate the connection of other data leading to breach of privacy through data

aggregation. All of which is likely to be further exacerbated by increased government gathering and processing of personal data.

Given the different ways organisations might act incompetently or unethically with data individuals attempting to keep culturally sensitive personal information offline may assume no aspect of their private life should be shared with public services, resulting in self-exclusion, widening the digital participation gap for certain minorities. While regulators should be able to use consumer data to better understand how people with protected characteristics can be better served, they will need to access such data in ways that do not undermine trust in authority. Regulators must engage with vulnerable groups and work with them to understand their concerns around the National Data Strategy and ensure they support new uses of their data.

Question 4

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

Below is the regional breakdown from our YouGov survey on public trust in the use of algorithms in public services. The survey question was "*Which, if any, of the following organisations do you trust to use algorithms to make decisions about you personally (e.g. benefits claims, educational, personalisation, credit decisions etc.)?*

*(Please select all that apply. If you **do not trust** any organisations to make decisions about you, please select the 'Not applicable' option)"*

The replies YouGov collected across the regions of England and devolved nations are shown in the table below:

	Total	Region								
		North	Midlands	East	London	South	England (NET)	Wales	Scotland	Northern Ireland
Base: All UK adults	2076	484	334	199	272	457	1746	100	174	56
The Government	10%	9%	12%	11%	9%	10%	10%	10%	11%	15%
Social media companies (e.g. Facebook, Instagram etc.)	8%	6%	7%	11%	12%	8%	8%	2%	12%	7%
'Big Tech' companies (e.g. Apple, Google etc.)	11%	8%	10%	13%	13%	11%	11%	5%	15%	10%
Financial services (e.g. banks, insurance companies etc.)	16%	13%	16%	14%	21%	18%	16%	7%	18%	15%
Health and social care (e.g. the NHS, private health care, the council etc.)	17%	13%	16%	15%	17%	19%	16%	14%	22%	21%
Armed Forces	7%	7%	9%	7%	4%	6%	7%	7%	12%	8%
The education sector	7%	6%	6%	5%	8%	7%	6%	4%	10%	6%
The police	11%	8%	12%	14%	10%	11%	11%	10%	15%	10%
Social Services	7%	5%	9%	7%	4%	7%	6%	5%	8%	13%
National Security and Intelligence services	12%	9%	11%	13%	11%	14%	11%	11%	17%	11%
Housing associations	6%	6%	5%	4%	5%	6%	6%	5%	8%	7%
Other	1%	0%	2%	2%	0%	1%	1%	1%	3%	-
Don't know	16%	18%	16%	17%	16%	13%	16%	21%	12%	21%
Not applicable – I do not trust any organisations to use algorithms to make decisions about me	53%	55%	55%	51%	47%	55%	53%	57%	48%	51%

This demonstrates the lack of public trust is uniformly low throughout regions in the UK, and it will be of critical importance for the National Data Strategy to focus on rebuilding public trust in all regions.

Question 5

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

Three key technologies can help improve productivity across all sectors, which are cloud based digital services, machine learning and big data analytics. According to the World Economic Forum these technologies are being adopted by the overwhelming majority of companies across all economic sectors, as shown in the following figure from the WEF 2018 report[18].

[18] http://www3.weforum.org/docs/WEF_Future_of_Jobs_2018.pdf

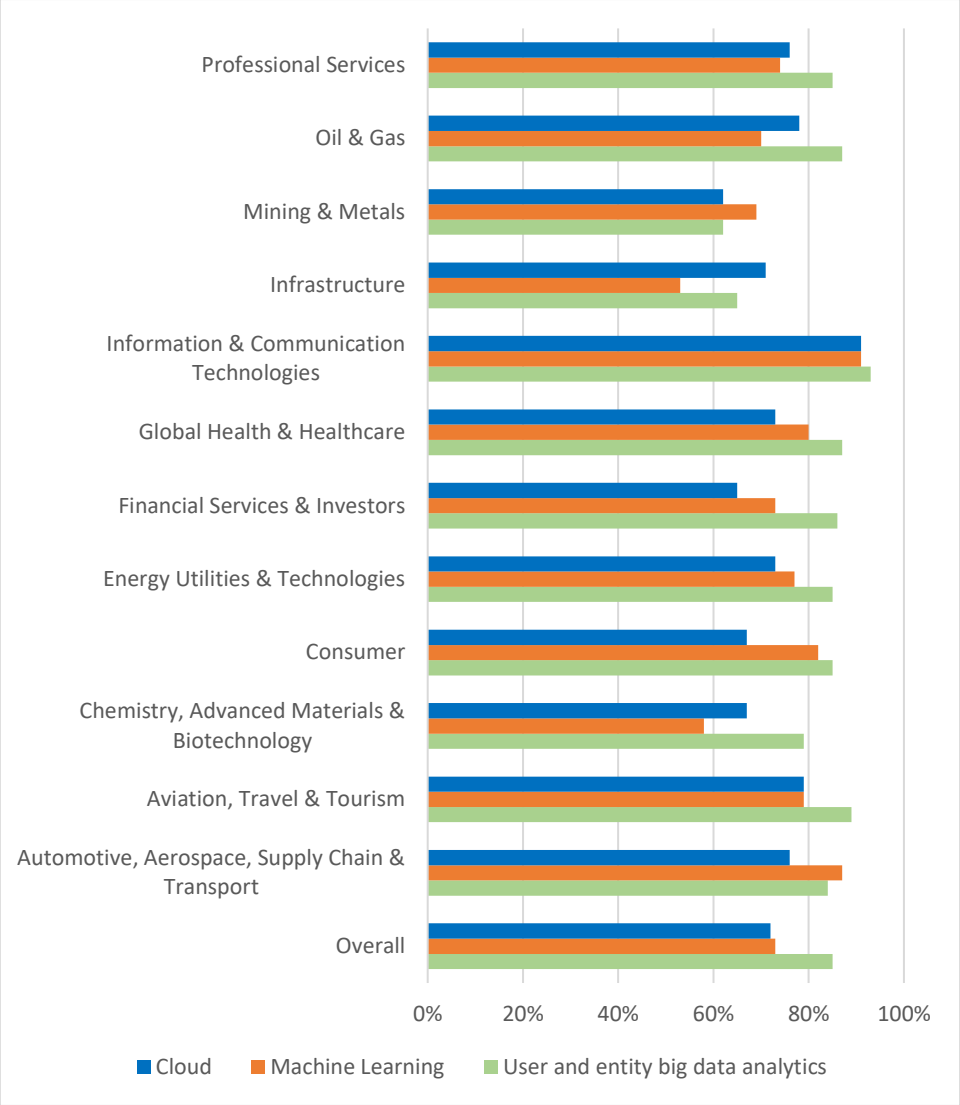

Figure 8: percentage of companies planning to adopt cloud, machine learning, and big data analytics technologies by 2022

Every sector will gain provided there are sufficiently many competent, ethical and accountable digital professionals working in those sectors. As outlined in the Executive Summary government should demand that digital professionals in all responsible positions are Chartered with an appropriate professional body to drive up standards across all sectors and should also galvanise the development of qualifications that are aligned with progression to Chartered status.

Question 6

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

As we explained in the Executive Summary it is vital for government to ensure there are enough competent, ethical and accountable computing professionals across all sectors to ensure the National Data Strategy is executed as rapidly and efficiently as possible.

Government should demand only professionals who are appropriately Chartered hold responsible roles in delivery of the Strategy in order to build public trust.

Question 7

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.

This question is answered by our Executive Summary. Essentially the Data Foundations pillar is underpinned by developing a sufficient supply of competent, ethical and accountable professionals across all sectors of the economy and underpinned by rebuilding public trust.

Question 8

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?

A particular barrier SMEs face is recruiting and training staff with appropriate skills. Government should consider how it can facilitate much greater numbers of digital apprentices in SMEs.

Question 9

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

BCS provided an extensive response to the Smart Data consultation and urge reviewers for this consultation to refer back to that document. BCS will be happy to provide additional copies of that earlier response if it would be helpful.

Question 10

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

Please refer to our Executive Summary for our response to this question. In particular government should focus not only on developing an appropriate data protection framework, but should also ensure the UK has sufficient competent, ethical and accountable digital professionals across all sectors to help develop and successfully adopt future data protection frameworks.

Question 11

Q11. To what extent do you agree with the following statement: the functions for the Centre for Data Ethics and Innovation (CDEI) should be Artificial Intelligence (AI) monitoring, partnership working and piloting and testing potential interventions in the tech landscape?

BCS strongly agrees with the above statement.

Question 12

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 which of these actions will have the biggest impact for transforming government's use of data.

Key to better use of data across government is the ability to develop trustworthy information systems that deliver maximum public benefit. To build such systems requires delivering each of the priority areas illustrated in the 'Trustworthy Stack' in Figure 9 together with an appropriate governance structure including all the stakeholder groups as shown in the figure.

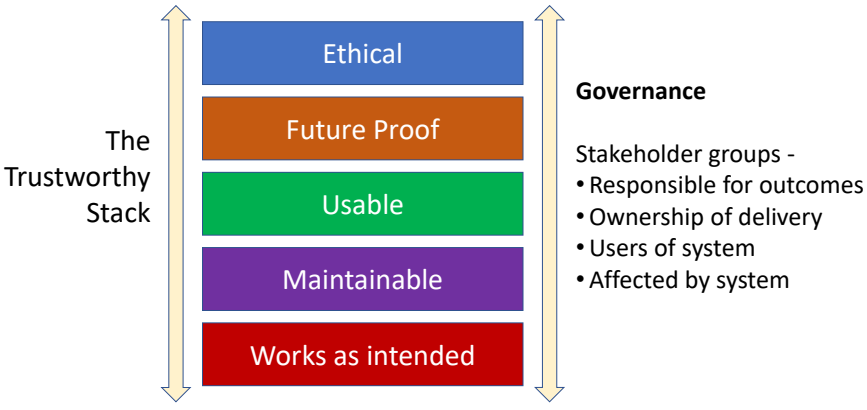

Figure 9: core elements for building information systems that enable better use of data

The key areas identified for action in the question map neatly into the different areas of the Trustworthy Stack. All of the action areas are necessary to deliver the full stack of trustworthy components. Moreover, they are all interdependent and are essential to delivering trustworthy public services in the sense of the above figure.

Question 13

Q13. The Data Standards Authority is working with a range of public sector and external organisations to coordinate or create data standards and standard practices.

We welcome your views on which if any should be prioritised.

We strongly recommend proactively consulting with professional bodies (not just computing professional bodies, but those such as management professional bodies with wider responsibilities). Understanding the practicality and utility of possible standards, developing standards that will work in practice, ensuring standards do not result in unintended consequences are all areas where engaging with a broad community of practitioners will be of great benefit. Professional bodies provide easy access to such communities and are effective at engaging with their communities to provide valuable input to standards development and implementation.

Question 18

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

Of immediate concern for the UK is the aftermath of the Schrems 2 legal judgment. The EU's 'Schrems 2' judgement ruled that the Privacy Shield Framework cannot be used for transferring personal data between the EU and US.

The Court of Justice of the European Union ruling has major and immediate implications for international flows of information as it says the current Framework does not match the EU's standards for protection of individuals' data. It will have sustained, post-Brexit impact on any countries that are not considered by the EU to have adequate data protection.

It has immediate implications for any organisation doing business by exchanging data and information flows with USA organisations, and for any organisation doing business by exchanging data and information flows with organisations based in countries the EU does not recognise as having an adequate data protection regime. All organisations are affected, from multinational to not-for-profit, to the extent that their data and information flows include personal data.

UK government should do everything possible and with urgency to remedy this situation. In addition, in the short term government should assist organisations with international data interests to take the following actions set out by BCS to minimise risk:

1. Assess how much of the personal data an organisation handles are strictly mission-critical and how much is expendable. Minimize an organisation's personal data. Be mindful that most business data are also personal data and that most datasets are mixed, and it may be impossible to segregate personal from non-personal data.

2. Assess in which countries personal data ends up routinely or occasionally, directly, or indirectly, via cloud services, web-based applications, cookies and other trackers, contractors, sub-contractors and suppliers. Map all the organisation's personal data flows you are responsible for against the interactive data protection map produced by CNIL. Keeping a real-time visual of how personal data ecosystem crosses national boundaries and of how data protection requirements for data transfers change will be useful also for upcoming changes in countries' data protection status. Consider whether transfer counterparts are a likely target for government intelligence surveillance demands.

3. Audit who has access rights to an organisation's personal data sets (databases, data streams, data repositories of any kind) and from which countries they can access it. Be mindful that, in legal terms, to access data is to transfer data. Include in this audit of permission levels: clients, business partners, employees, remote workers, freelancers, temps, interns, volunteers.

4. If there is an in-house legal department, they should have reached out to the IT team by now. If an organisation uses external legal counsel , they may not have made contact yet, so be proactive: re-read your own policies and search the terms and conditions of your suppliers, contractors and subcontractors to identify which data flows in your organisation rely, directly or indirectly, on a "Privacy Shield" clause . This is a legal basis for transferring data to the USA that is now invalid. Do the same search for Standard Contractual Clauses (SCC). These are still valid but require additional action on your part. For example, to continue to use SCCs you will need to undertake due diligence to evaluate and document the risks associated with those transfers. In practice, you will need to identify if the laws of the destination country cause concern in relation to the rights of data subjects (see action 2). To identify potential risks, an assessment of the third country’s laws and potential international commitments is now necessary and recommended by the EDPB. You should also ensure the data importer in the destination country understands that it needs to notify you of laws and other obligations that would prevent it from complying with the SCCs, including being subject to any specific government surveillance or legal monitoring.

5. Address highest risk transfers first. For example, a financial institution is likely to have high levels of risk, whereas a small online retailer is likely to have lower levels of risk of surveillance interception. Where it is possible that US governmental authorities might seek to access the personal data transferred, consider including additional protections, such as encryption or tokenization, which could render personal data meaningless to a third party, or adding suspension or termination clauses in contracts that allow the data exporter to minimise the risk of an enforcement action in the EEA and the threat of fines.

6. Once you have quantified the amount and kinds of personal data transfers to the USA, servers controlled by US companies or other countries outside the European Economic Area (EEA) which do not provide adequate safeguards, escalate the matter to the highest level of risk ownership in your organisation.

7. Be in the room when management works out the cost-benefit analysis of practical solutions for the parts of your business that rely directly or indirectly on Privacy Shield or SCCs. There may be several solutions. None is without consequences. Go to the meeting prepared to offer key figures of data transfers, and your assessment of IT architecture workarounds.

8. IT additional safeguards or alternative IT architecture workarounds may not be the only solutions to Privacy Shield-based data transfer to the USA or those data transfers based on SCCs:
   a) Business alternatives include redesigning which type of business processes are carried out by which country's business unit or switching to cloud and other IT suppliers which are not subject to US jurisdiction.
   b) Legal alternatives include replacing Privacy Shield with SCC with "additional safeguards" as the legal basis for transfers or relying on one of or more of the specified "derogations" in Article 49 of the GDPR or, in the case of multi-national organisations, considering the use of Binding Corporate Rules (BCRs).

   c) IT alternatives include re-allocating personal data access privileges to staff in the EEA, arranging for the business' personal data be processed exclusively by staff based in the EEA, adding encryption layers and ensuring encryption keys are in your possession, pseudonymising or anonymising personal data.

9. Continue to monitor developments. The interpretation and application of Schrems 2 is rapidly changing and developing.

10. Work with colleagues and professional communities to influence positive change.

Who we are - BCS, The Chartered Institute for IT

BCS is the UK's Chartered Institute for IT. The purpose of BCS as defined by its Royal Charter is to promote and advance the education and practice of computing for the benefit of the public.

We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

As the professional membership and accreditation body for IT, we serve over 60,000 members including practitioners, businesses, academics and students, in the UK and internationally.

We also accredit the computing degree courses in ninety eight universities around the UK. As a leading IT qualification body, we offer a range of widely recognised professional and end-user qualifications.