

Open Rights Group are grateful for the opportunity to provide our input on the National Data Strategy consultation. Open Rights Group are a digital rights campaigning organisation. We seek to help build a society where rights to privacy and freedom of speech online are respected, protected and fulfilled. We have over 20,000 engaged supporters across the United Kingdom. We advocate evidence-based policy, guided by respect for fundamental human rights.

We thank DCMS, the Ada Lovelace Institute, and the ODI for consulting with ORG directly and through workshops in advance of this consultation response, and for taking our comments and considerations on board as the dialogue around the Strategy has evolved.

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.

We somewhat disagree with this statement.

ORG generally agrees with the pillars which the Strategy has identified to promote the better use of data. However, we find reasons to be concerned about some of the contents of the mission.

The fundamental problem with the National Data Strategy is that it is a political strategy about data which works from the position that data is not political. It views data as sterile and factual strings which exist in a vacuum and are used in a purely technical manner. History and lived experience, both distant and recent, teach us otherwise. It is that historical legacy which has given us the data governance systems we live with now, as well as the rights-based approach which underpins them.

The UK currently enjoys high standards of data protection and privacy rights which have come to us through the European data protection regime. These rights are covered by oversight, transparency, and redress for misuses and abuses of data. At times, however, the Strategy characterises regulation as an obstacle to innovation (see for instance, “securing a pro-growth and trusted data regime”).

To preserve these standards and rights, we do not want to see the Strategy co-opted into a vehicle for a vague, ill-formed, and zealous deregulation agenda. Any alterations to existing data law, whether through this Strategy or outside it, must preserve and, indeed, enhance our existing individual data protection rights and privacy standards. Those alterations must also consider the role,

remit, efficacy, and enforcement powers of the data protection regulator (the ICO).

Regulatory safeguards, oversight, transparency, and an effective liability regime should be seen as the key elements to unlock the “value of data”, rather than any technical innovations per se.

The recent A-level failure should constitute a warning of what happens when those safeguards, checks, and balances are considered optional or, perhaps, a form of bureaucratic excess. When individuals feel unfairly treated, powerless to do anything about it, and without effective redress, public trust in government use of data is easily lost and not easily restored. The damage done in this instance, which rendered an entire generation with feelings of alienation from “the algorithm” and the government system around it, will adversely impact their trust in public use of their data for life.

Whether the “value of data” can be fully realised or not is dependent on developing legal, organisational and human capacity, not technical innovations and standards. This work requires integrity, transparency, and public support, not to mention a significant investment in resources and funding.

In treating safeguards and regulation as a barrier, the mission outlined by the National Data Strategy risks undermining trust, exacerbating power imbalances, and enabling discrimination. All of those risks can be easily mitigated, if government so chooses.

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.

As we finalised our response to this consultation, we learned of an investigation into UK councils using “data, predictive analytics and artificial intelligence” to create algorithmic scores of private households who “are believed to be vulnerable” from Covid-related disruption.¹ The investigation also showed that this system was sold to councils specifically to help them identify households who the system deemed at risk of breaking lockdown restrictions:

“The information is culled from council records and includes family debt levels, living arrangements, income, school absences and exclusions. It is fed into a profiling system called Covid OneView to create a risk analysis for households and individuals who are believed to be vulnerable...

A separate briefing note last month noted how councils could further harness data from the documents provided by 'drilling down' into a 'breadth of categories' and find extra details to be included for analysis. These included 19 'high level' classifications, including socially unacceptable behaviour such as 'unfaithful and unsafe sex', and hazards and threats, which included being 'potentially aggressive', or having dangerous pets.”

The Covid OneView system was deployed without the consent or knowledge of the people whose data was contained within it. It was deployed in a manner which is neither necessary nor proportionate, making sweeping judgements about whose data goes into the system in the first place and what conclusions could be drawn from it. It almost certainly includes data culled from third party sources with no relevance whatsoever, such as dating apps. It has been put into place without the legally required data rights (the right to be informed, the right to dispute the data, the right to object to automated and algorithmic processing, and the right to order that their data be removed from the system) being provided to the people being studied.

¹ <https://www.dailymail.co.uk/news/article-8994911/Town-halls-harvest-millions-personal-details-including-youre-unfaithful-debt.html>

This system is clearly an egregious violation of personal privacy, an abuse of private and public data, and a pointless waste of taxpayers' money. However, the Covid OneView system is also an example of the kind of data uses which this Strategy seemingly seeks to achieve to facilitate.

The simple fact is, if government cannot take a proportionate, rational, and legally compliant approach to data use under the legal and ethical constraints which already exist, we do not see how the Strategy could possibly improve on that situation if it does not put those principles front and centre.

Rather than brainstorming new innovations - which are more likely than not to lack guardrails and constraints - for data, using the pandemic as a cover, government must bring these practices to a hard stop and go back to the basics. This starts with process and transparency. We agree with the ODI/Ada Lovelace Institute suggestion that "Different assessment components, such as data protection, algorithmic equalities and human rights impact assessments, could be combined into one process under the umbrella of DPIAs, as prescribed by the General Data Protection Regulation (GDPR)"². It is a useful creative exercise to consider how the OneView system's abuses of data would have been mitigated, or not permitted to happen at all, had that enhanced process taken place.

Process and transparency must include all levels of government, from cabinet down to local authorities, and should be given adversarial scrutiny, rather than a friendly rubber-stamping, by the data protection regulator.

² <http://theodi.org/wp-content/uploads/2020/11/Getting-data-rightperspectives-on-the-UK-National-Data-Strategy-2020.pdf>

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

As we discussed in Q1, the National Data Strategy works from the position that data is not political. This is not, and has never been the case, particularly for marginalised, excluded, and legally diminished communities. In that regard, we are greatly concerned that the Strategy neither acknowledges the power dynamics which exist around data, nor recognises the structural inequalities it is likely to exacerbate.

We need only look at the impact of the immigration exemption on the take-up and usage of COVID apps by minority and migrant communities.³ These groups are neither downloading nor using COVID apps, nor reporting their symptoms to the NHS, because the immigration exemption means there are no legal safeguards in place to prevent their data from being used against them. In a public health emergency, it is simply staggering that members of the public - who, we must note, are here legally - are having to opt-out of the public health system because they do not enjoy the same protections which cover others, simply because of who they are.

Furthermore, there are other examples, ranging from the PREVENT strategy to suspicionless “stop and search” to the Home Office’s racist visa algorithm⁴ (which was found to be in violation of the Equality Act), which demonstrate precisely why many communities maintain a hostile approach to information gathering. What government paints as benign attempts to empower the uses of data under the Strategy will only ever be seen as leverage to persecute and condemn.

Data is meant to inform decision-making through assumptions and correlations. This will always carry the risk of unfair or wrong decisions being made as the result of an individual diverging from the intention of the data use. It is therefore pivotal for the uses of data which are about (or are being used to inform decisions about) minorities, people from disadvantaged backgrounds, or people who are just quite simply different from the average must not be detrimental. This can be achieved by enhancing legal and ethical requirements for fairness, transparency, and access, and by increasing external and regulatory scrutiny.

These obligations must apply to anyone accessing public data, including private contractors and arms-length organisations. There can be no exceptions

³ <https://www.openrightsgroup.org/blog/data-trust-will-migrants-use-the-nhs-app/>

⁴ <https://www.bbc.co.uk/news/technology-53650758>

to safeguards, and anything which takes away from those safeguards must be removed, whether that is a negative (e.g. the diminished rights under the immigration exemption) or a positive (e.g. the increased information gathering and surveillance powers which the exemption gives government bodies).

Further safeguards in this regard could be given by establishing an effective liability regime for automated-decision making which go beyond GDPR and its requirements for human review.

Until those inequalities are acknowledged, safeguards and guardrails are established, and government understands the privileges with which it views access to data, the Strategy can only ever be a strategy for some and not for all.

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.

When considering regional inequalities, we call your attention to a critical and overlooked issue: the island of Ireland and data. These are issues over and above EU data protection adequacy which have been entirely ignored thus far. This situation involves the complex interplay between GDPR adequacy, the Law Enforcement Directive, the Withdrawal Agreement, and the Good Friday Agreement. The lack of attention to the consequences of this interplay has raised the real and substantial possibilities that data processors and controllers, on both sides of the border, may need to run double data protection systems, going so far as to segregate data strings within a single data record. The legal and practical risks to both Irish and Northern Irish businesses have barely been considered:

*For a start, all RoI (or other EU MS-based) businesses that regularly exchange personal data with NI businesses (and many state agencies that are subject to the GDPR) will have to use standard [data transfer] contract clauses (SCCs) (or BCRs if they are in a group with the other business, or for data transfers between public entities, administrative agreements) PLUS “supplementary measures” as just clarified by the EDPB. **Those supplementary measures must effectively prevent the UK security agencies from unduly accessing the transferred data.***

*What is more, if the RoI (or other EU MS-based) business concludes that there are no “supplementary measures” available that will actually prevent access to the personal data in NI (or the rest of the UK) by the UK security and intelligence agencies, then they are **legally barred from transferring the data.***

*If in spite of this conclusion, they nevertheless still want to transfer the data, they are **legally obliged to consult the relevant national data protection supervisory authority** (i.e., in the RoI, the Irish Data Protection Commissioner) – and the supervisory authority is obliged to **prohibit the transfer** if indeed the data cannot be protected after transfer against undue access by the UK authorities.*

It gets worse still: the EU GDPR also applies to non-EU/EEA controllers or processors who “offer goods or services” to individuals in the EU/EEA (in some targeted way)– so NI businesses that after 1 January (also) offer their goods or services across the border will still be subject to the EU

GDPR, as well as to the UK GDPR. The same applies if they “monitor the behaviour” of individuals in the EU (including in the RoI), e.g., by using tracking tools on their website.

That also means that such businesses are prohibited, under Article 48 GDPR, from complying with any UK court judgment, or any decision of any UK administrative authority, in respect of the personal data that they process in relation to the offering of goods or services to EU (including RoI) persons, or in relation to the monitoring of the behaviour of such persons.⁵

Government should, as a matter of urgency, allocate resources to establishing legal certainty on data flows and adequacy across the Irish border from 1 January, working from the position of safeguarding the Good Friday Agreement first and foremost, and ensuring any data-related outcomes second.⁶ UK and Irish data protection regulators must also be prepared to provide guidance and support to businesses which may find their data processing operations severely disrupted, including assistance in creating legal bases for continued data transfers, and the ICO should devote resources to the task.

⁵ <https://www.ianbrown.tech/2020/11/13/data-protection-and-data-transfers-on-the-island-of-ireland-after-the-post-brexit-transition-period/>

⁶ <https://neweconomics.org/2020/11/the-cost-of-data-inadequacy>

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

Data, when correctly used, can benefit any sector of society. However, this also means that its potential to harm or benefit individuals does not depend on the sector in which it is being used. Hence, it is imperative that the UK maintains a robust rights-based legal framework to protect individuals against adverse uses of their personal data.

Furthermore, as the boundaries between personal and non-personal data grow ever thinner, the UK should consider extending some of the safeguards for the processing of personal data to non-personal data. This also includes maintaining a broad and flexible definition of what personal data is, and extending the data rights available to data subjects.

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

Government's role should be to establish and shape guardrails and constraints against the unlawful and/or harmful use of data. It can do this through preserving, enhancing, and enacting privacy and data protection legislation. It must also strengthen and enhance regulatory oversight and enforcement of data protection law.

Effective regulation improves transparency, accountability, and the effectiveness of redress options for individuals who suffered abuses of their data. It also discourages public and private actors from relying on data for the wrong reasons, such as discrimination, or the willingness to elude responsibility.

Government's role in enabling better availability of data must be viewed from a positive perspective - in other words, what can they add, such as security standards or requirements for algorithmic transparency - rather than a negative perspective of what they can take away, including any post-Brexit deregulatory rush for weaker standards and watered-down constraints.

Government should also consider public procurement, as well as openness of non-personal data created through public funds, as a way to promote higher standards for data protection, security, and fairness in the use of data.

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.

The definition of "data foundations" in this question concerns format. The semantics of data can easily be standardised. Accountability cannot. We would therefore encourage government to lead here by focusing on establishing foundations for data transparency and accountability, rather than file formats.

An obvious way to do this would be to legislate for open data in every new piece of legislation, and to ensure a transparent data protection impact assessment accompanies any new law, just as a regulatory impact assessment would. Enhanced data protection impact assessment processes, as we discussed in question 2, should also come into play.

We would caution, however, against viewing the establishment of data foundations as a means of paving the way for open government data to be sold as an asset. Public trust in government will evaporate quickly if the data they thought was collected in their interest is, instead, repurposed for profit. And the public will not blame any resulting adverse impacts from the use of data on the third parties which misused it; that blame will be laid solely on government's doorstep.

Particular care must be taken over children's data, which is often collected by government and educational bodies in a disproportionate, non-consensual, and often highly intrusive manner under the label of safeguarding. Foundations for children's data must consider these ethical, legal, and technical aspects in even greater depth and detail than regular uses of data, with an understanding that you do not find a needle in a haystack by making the haystack bigger.

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

The UK's data protection framework, which stems from GDPR and PECR, establishes adequate and proportionate protections over the processing of personal data. That European-derived framework has already become the global standard for upholding personal privacy rights, as well as providing legal certainty for companies which use personal data.⁷

What has not proven fit for purpose has been regulatory enforcement of that data protection framework by the ICO. The perception of the UK as a country with weak oversight, if not an outright blind eye to abuses of data, has contributed to the growth of misleading or coercive practices to circumvent the law.⁸ It is not for nothing that the ICO's lax enforcement has now become a Parliamentary concern, with a DCMS committee hearing scheduled for January.

Many practical routes are available to improve overusing and enforcement, and in turn, ensure the UK's data protection framework remains fit for purpose. These could include

- Setting clear statutory limits regarding the progress of complaints;
- Clarifying communication and transparency duties for the ICO when dealing with interested parties during the course of investigations;
- Introducing collective redresses mechanisms – for instance, by implementing article 80(2) of GDPR into the Data Protection Act 2018; and
- Improving resourcing. More data use requires more oversight, and this must be properly financed and resourced, both at the data governance and law enforcement levels.

Finally, the international dimension of data transfers requires cooperation and alignment. As such, the UK should strive to obtain and maintain an adequacy decision with the EU, which we will discuss in question 18.

⁷ https://www.cisco.com/c/en_uk/products/security/security-reports/data-privacy-report-2020.html

⁸ <https://www.accessnow.org/cms/assets/uploads/2019/07/One-Year-Under-GDPR-report.pdf>

Q11. To what extent do you agree with the functions set out for the Centre for Data Ethics and Innovation (CDEI) - AI monitoring, partnership working and piloting and testing potential interventions in the tech landscape? Please explain your answer.

While we agree that the CDEI could play a role in facilitating new approaches to data use outside a traditional legal compliance context, we are concerned that the Strategy prioritises the work of the CDEI (data ethics) over the work of the ICO (data law) to the point that it risks engaging in ethics washing.

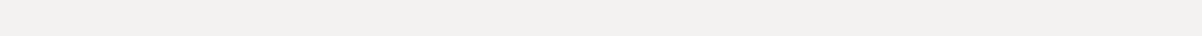
“Ethics washing” is an academically recognised phenomenon, largely centred around privacy law and regulation, where ethics projects are deployed in lieu of a legal compliance. These initiatives are rarely deployed to complement privacy laws and the rights they grant users; instead, they are often used to circumvent them, while justifying the ensuing results as “ethical”. In government environments, where all uses of data can be justified one way or another as being in the public interest, the risk of ethics washing is even greater than in the private sector.

We were heartened by answers given to us by DCMS during the ODI workshop⁹ indicating that they had no intention of replacing or supplanting the ICO’s legal oversight with the CDEI’s ethical guidance, or to watering down the legal safeguards which the ICO enforces in favour of non-binding CDEI codes of ethics. This should carry over into practice in ways that ensure that the two organisations are not, in actual fact, developing separate approaches to privacy which would allow data misuse to be justified, if not selectively chosen, by those who would misuse it. To achieve this, we would like to see steps taken to ensure that the two organisations engage in regular checks and balances, and that they “walk the walk” by demonstrating public transparency which will allow for external scrutiny.

A starting point for these checks and balances would be the “six tests” developed by Ben Wagner at the University of Vienna¹⁰ to check that any work the CDEI carries out, in a data strategy context, is not in fact a form of ethics washing:

⁹ <http://theodi.org/wp-content/uploads/2020/11/Getting-data-rightperspectives-on-the-UK-National-Data-Strategy-2020.pdf>

¹⁰ https://www.privacylab.at/wp-content/uploads/2018/07/Ben_Wagner_Ethics-as-an-Escape-from-Regulation_2018_BW9.pdf

- 1) There must be early and regular engagement with external stakeholders;
 - 2) There must be a means of external, but not necessarily public, independent oversight;
 - 3) There must be transparent procedures on why choices were made;
 - 4) There must be a stable framework of non-arbitrary standards which can be used to reference the selection of certain values, ethics, and rights over other ones;
 - 5) There must be a clear indication that the elected ethics do not substitute for fundamental human or citizen rights;
 - 6) There must be a clear statement on the relationship between the principles declared and any existing legal or regulatory frameworks, including an explanation of what will happen if the principles and the law are in conflict.
- 

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.

Quality, availability, and access

The development of a coherent Strategy for data is no doubt positive, and should be encouraged. However, as we considered the Strategy, we found that many of the suggestions raised within it already exist as part of legal requirements. These include the quality and accountability principles of data protection, in addition to transparency and enforcement of rights. In that light, we are concerned that the Strategy leans towards presenting a binary narrative of innovation vs. regulation, rather than considering how existing data protection law can be leveraged to increase trust and accountability.

We encountered many of the issues raised in the Strategy during the development of the Digital Economy Act 2017, which created new powers and mechanisms to increase data sharing in the public sector. The relative lack of impact of these powers deserves better scrutiny before potentially asking for another set of reforms.

Capability, leadership, and culture

In a data governance context, 'Capability, Leadership and Culture' are not about sowing the seeds for risk-taking innovation, but are about the skills needed to use accountability frameworks to make responsible data use an everyday practice.

Government data policy was moved back to the Cabinet Office in July. We note that the Cabinet Office ran a very encouraging exercise in the lead-up to the Digital Economy Act 2017 to work with stakeholders, including civil society. This open policymaking led to the introduction of new permissive legal powers for various government departments to increase data sharing, as well as

concrete safeguards. The powers granted to public services were clearly tied to benefitting end users, and powers for fraud and debt were given sunset clauses and pilots.

However, the powers have not resulted in the expected results. A mid-term report on the use of these powers from February 2020 showed that with the exception of fuel poverty, the data strategies designed to help people in need have barely been used. In contrast, the data strategies designed to help government administration, such as civil registration, fraud and debt have been extensively used. The amounts involved in fraud particularly are not very high, however. These powers operated on a pilot basis with a sunset clause pending renewal.¹¹

A report from April 2019 for DCMS¹² showed that the powers under the DEA for public sector delivery were not being used as much as expected. This was due to perceived complexity, a lack of awareness in major data holding departments, concerns about GDPR (which were found to relate to lack of information), and alleged limitations on the use of health and social care data. A lack of leadership was also stopping data sharing.

This report shows that many of the obstacles to data sharing are in fact cultural and do not require legal changes. However, this also shows that the ask for that cultural change is not so much to promote a risk-taking culture of sharing-by-default, but to work through the legitimate concerns and issues faced by the civil servants involved. Cultural perceptions also included a reluctance to be transparent and open, linked to fear of repercussions.

Standards and assurance

The DEA powers were expected to streamline data sharing, ending “zombie gateways” and bringing more transparency. There are registers for data sharing under the powers,¹³ but more broadly, transparency on sharing is limited. Some department have registers but without enough information to know what is being shared.¹⁴

Other ideas proposed at the time, such as creating personal data dashboards for individuals to know where their data is held, have come to nothing.

11 <https://www.gov.uk/government/publications/digital-economy-act-2017-part-5-codes-of-practice/mid-point-report-on-use-of-the-dea-powers#updates-on-use-of-the-information-sharing-powers>

12 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/895505/_Kantar_research_publication.pdf

13 <https://registers.culture.gov.uk/>

14 <https://data.gov.uk/dataset/8f241d90-3c60-4b8e-a28b-fa5ffe7a87af/data-sharing-register/datafile/77b8758a-23fd-490d-a3f2-114e9f222752/preview>

Accountability and productivity

Accountability is the most important area of practice, but what seems to have taken place in recent years is that processes have been confused with progress. In that light, the first step towards a more accountable data strategy should be improving existing processes rather than adding new ones.

For example, among the safeguards in the DEA are review boards, but their impact appears to be mixed:

- The Public Service Delivery Review Board has met four times in two years. The minutes from the first meeting¹⁵ show that the board had many questions and requests to make their work impactful, but it is unclear many of those have been implemented. The board appears to only have considered one data sharing project.
- The minutes of the review board for fraud and debt¹⁶ show that there are many pilot projects sharing data in those areas. The need for more powers is not clear.
- The PSD review board¹⁷ discussed bringing health data within the remit of the DEA through NHSX, leading to public concerns, and showing the sensitivity of the topic that initially led to its exclusion.
- The Law Commission produced a comprehensive review of data sharing¹⁸ in 2014, which was ignored by the government at the time. The report recommended a full legal reform project with extensive mapping of existing arrangements and extensive training and guidance.

These underwhelming results have benefited no one. The Strategy should avoid adding more mechanisms - and job creation schemes - and focus on improving what exists instead.

Ethics and public trust

Public trust on the government's ethical handling of data is quite low, at around 30% in some surveys.¹⁹ Government can only improve on this trust

15 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795513/20180925_-_PSD_Review_Board_minutes__1_.pdf

16 <https://www.gov.uk/government/publications/the-digital-economy-act-2017-debt-and-fraud-information-sharing-review-board>

17 https://www.theregister.com/2020/03/09/uk_government_medical_data_sharing_plans/

18 <https://www.lawcom.gov.uk/project/data-sharing-between-public-bodies/>

19 <https://theodi.org/article/nearly-9-in-10-people-think-its-important-that-organisations-use-personal-data-ethically/>

through actions and not words.

It can start with transparency, which is a requirement under data protection law. Government can go beyond the legal requirements of data disclosure to provide more information than is strictly required. Unfortunately, in recent years, government has retreated on wider transparency efforts, ranging from FOIA to open government and policy making. In that light, the aims of the Strategy are at odds with the reality.

Additionally, we note that one of the legal bases for use of data is consent. Trust cannot be confused with consent. The use of consent in the public sector is challenging, because due to the power of the state, it can rarely be seen as freely given and consensual. The exemptions from consent requirements which exist within data protection law when data is used for public and government administration purposes must not be confused with open consent, much less trust in government to use that data.

Q18. How can the UK improve on current international transfer mechanisms, while ensuring that the personal data of UK citizens is appropriately safeguarded? We will seek EU 'data adequacy' to maintain the free flow of personal data from the EEA and we will pursue UK 'data adequacy' with global partners to promote the free flow of data to and from the UK and ensure it will be properly protected.

Where international transfer mechanisms are concerned, the UK cannot have its cake and eat it too. The European standard of data protection adequacy, by design, creates a duty to ensure that adequacy is agreed only where countries also recognise only other countries with sufficient standards for data transfers. *Government must understand that any commitment it enters into with other nations for a lesser standard of data protection, by definition, could risk its European adequacy, or force the UK to develop a two-tier system of data management.*

Currently, there is a well developed international system for adequacy, and one which is growing. This is both improving global data protection and providing for the greater free flow of data. It would be foolish to move away from a system that is delivering both rights and data flows, especially when these are the Government's stated policy aims. Government must clarify how it intends to maintain a level playing field on data privacy, for its own citizens and for its trading partners, when the only other choice is a race to the bottom.

In this regard, we would also ask government to consider the risks associated with inserting data protection and flows into the UK's trade deals. The UK-Japan trade deal may expose the UK's adequacy system to future legal challenges. These risks come from articles which place limits on government action to restrict data flows to that which is "necessary". The EU, for instance, has concluded that it should not agree such articles, as they pose a risk to their system of adequacy. Such articles also appear in the CPTPP framework.

These risks to existing and future data protection safeguards were agreed in the Japan agreement without Parliamentary and civil society scrutiny, and should stand as an example of practices which should not be repeated. An analysis of these articles from an international law perspective is urgently needed, beyond assertions that they pose no risk.

Continuing to payload privacy and data issues into future trade deals, in addition to jeopardising personal privacy, will also lessen the UK's international standing as a nation which views digital and human rights as the outcome of inclusive processes involving multiple stakeholders and levels of society. A trade deal which "goes it alone" on data protection, in every sense, does not a desirable trading nation make.

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?

In order to ensure the best possible outcome for the UK in future adequacy arrangements, the UK must first define what privacy principles it intends to stand for as an independent nation outside the EU. That process must start from the position of preserving, protecting, *and enriching* personal privacy rights. However, four and a half years after the UK voted to leave the EU, we have yet to hear anyone - at all, in either government or the private sector - discuss Brexit as an opportunity to do that. The dialogue is, instead, focused on deregulation and the removal of rights – risking throwing out the privacy baby with the EU bathwater.

This Data Strategy should be the start of a positive and supportive dialogue to counter that rhetoric. Government should also consider that data adequacy should not be viewed solely through the lens of data protection law. We should consider how our potential trading partners protect digital rights in other ways, such as ensuring algorithmic transparency, respecting freedom of speech, and supporting robust intermediary liability principles, in ways that do not create supplementary threats to data rights. These principles should be documented and evaluated using the enhanced processes we discussed in Q2.

There is an imminent opportunity to put this new approach into play. As the US moves towards an inevitable Federal-level privacy law in 2021, the UK has an opportunity to show leadership and diplomacy in helping the US to overcome its cultural, historical, and political discomfort towards privacy, and to recognising privacy as a fundamental human right - a right which is well overdue for US citizens. Supporting the US to step up to a “starter” standard of privacy, as opposed to the UK *stepping down* to the US’s level, will be a well-received gesture for a nation not ready for the European privacy model, and will also benefit the personal privacy of UK citizens who depend on US services. This will be a rare opportunity to build a new scaffolding to support data, human, and privacy rights. The UK should work with the EU and other countries with strong data protection systems such as Canada and Japan to promote this.