CIPL's response to the UK National Data Strategy Consultation

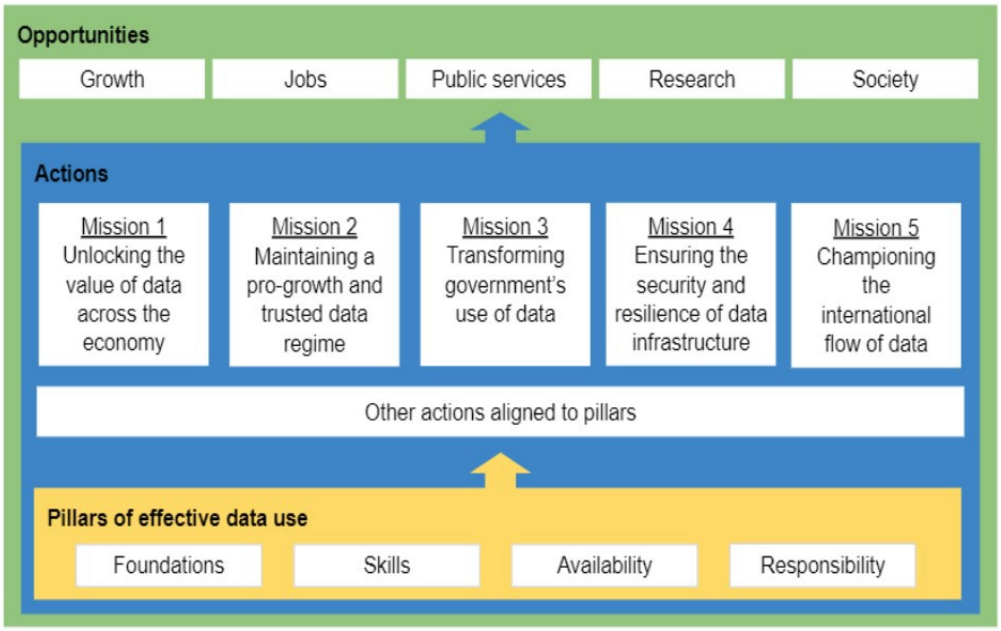
by the Department for Digital, Culture, Media and Sport (DCMS)

Submitted online[1] on 2 December 2020

Overall

We want to ensure that we produce a forward-looking strategy that takes into account public opinion and delivers real change. These questions will help to inform future work that the government will take in this space. They will provide evidence for the government to target areas for intervention in future policy.

Please find a diagram below of the NDS pillars, missions and opportunities for reference.



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

Please explain your answer here and, if applicable, identify any areas you think the government should explore in further depth.

The Centre for Information Policy Leadership (CIPL) strongly agrees with the, mission, pillars and priorities set forth in the UK National Data Strategy. While it was clear before, the need for unlocking the value of data, including through data sharing between and among public and private sector organizations during the COVID-19 pandemic, has further confirmed that data is a fundamental building block of modern society and a critical asset for the wellbeing and prosperity of mankind, innovation, the economy and public and private entities. Data also fuels the development of Artificial Intelligence (AI), and makes data sharing and ensuring the availability of data a critical component of the UK's digital strategy. CIPL appreciates the UK government's effort to create a strategy

[1] https://www.gov.uk/government/consultations/uk-national-data-strategy-nds-consultation/uk-national-data-strategy-consultation and https://www.smartsurvey.co.uk/s/NDS2020/.

that aims to increase the use of, and demand for, data and data-enabled products and services. CIPL further commends the UK for considering the strategy through a holistic lens and addressing aspects, such as the quality and availability of data, opportunities to use data for social and economic good, market power and data for small and medium enterprises (SMEs), interoperability between data protection frameworks, cross-border data flows, data infrastructure, digital literacy and data protection and cybersecurity. In this context, it is particularly important to devise an appropriate regulatory model (laws, regulations and regulatory oversight) that supports and incentivizes innovative and accountable uses of data.

We commend the work of Professor Christopher Hodges, Professor of Justice Systems, Centre for Socio-Legal Studies, University of Oxford, who studies trends and models in modern regulation and who has articulated forward looking regulatory approaches that emphasize value, evidence, motivation, cooperation and trust and de-emphasize deterrence and enforcement, reserving those aspects to law violations that are serious, intentional, reckless or the result of gross negligence.

See the following: (1) Delivering Data Protection: Trust and Ethical Culture, Christopher Hodges (2018), available at https://bit.ly/3pdSFh2, (2) How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner? A Reaction to Christopher Hodges, Hielke Hijmans (2018), available at https://edpl.lexxion.eu/article/EDPL/2018/1/10, and (3) Ethical Business Practice and Regulation: A Behavioural and Values-Based Approach to Compliance and Enforcement, Christopher Hodges and Ruth Steinholtz (December 2017), available at https://amzn.to/36j3k1p.

In addition, CIPL has applied the findings of Professor Hodges and others in behavioral economics to data protection regulation and issued a white paper on effective data protection regulation based on this model.

See the CIPL Regulating for Results white paper: Regulating for Results: Strategies and Priorities for Leadership and Engagement (October 2017), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement_2_.pdf.

Incorporating the approach set forth in these materials will support each of the five missions set forth in the UK National Data Strategy, in particular Mission 2 to maintain a pro-growth and trusted data regime.

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.

For a detailed discussion on the impact of COVID-19 on data uses for new and beneficial purposes and the public good, please see CIPL's June 2020 white paper on Looking Beyond COVID-19: Future Impacts on Data Protection and the Role of the Data Protection Authorities, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_remarks_-_looking_beyond_covid-19_-_future_impacts_on_data_protection_and_the_role_of_data_protection_authorities__2_june_2020_.pdf, This paper includes examples of data uses for health and public welfare-related purposes, but also employment purposes, business continuity purposes, social impact (data for good) and other purposes. To the extent such uses would benefit from and accelerate through data sharing between and among public and private sector entities, the government could help develop frameworks that enable such accountable and trusted data sharing. It is also important that the Government addresses the way in which the UK Data Protection Act 2018 is being implemented and functioning. This should ensure there are no misconceptions regarding the interpretation of its rules. It will also reduce the existing reticence risk of organizations, both in private and public sectors including SMEs and start-ups, not embarking on data sharing and data innovation activities for fear of breaching the UK Data Protection Act 2018 and being subject to draconian GDPR fines.

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 (https://www.equalityhumanrights.com/en/equality-act/protected-characteristics) under the Equality Act 2010?

CIPL has advocated for a risk-based and accountability-based approach to the use of personal data. This approach essentially would require all organizations using personal data to have comprehensive privacy and data governance management programs in place that ensure full compliance with and operationalizes all applicable legal requirements (including anti-discrimination laws). Risk assessment is one of the key elements of accountability and requires organizations to assess the risks of harm associated with data processing, as well as the benefits and purposes of processing, and to implement mitigations for any identified risks of harm. Such risk assessments would include assessment of the risks associated with processing data reflecting protected characteristics and would require that the identified risks would be specifically mitigated to prevent discrimination. We believe the concepts of accountability and risk-based approach are relevant for all areas of digital and data regulation, beyond personal data and data protection only. We recommend that the risk-based and accountability-based approach be incorporated into the UK's digital and data strategy, including specifically in respect to the development and use of AI and data sharing. The GDPR and the UK Data Protection Act 2018 already incorporate both accountability and risk-based approach. They should be further emphasized and elaborated upon both in the application of the UK Data Protection Act 2018 and in other UK data related rules, regulations and co-regulatory frameworks.

For more detailed discussions of this topic, please see the following CIPL white papers:

CIPL Risk Paper—Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR (December 2016), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.

CIPL/Hunton Andrews Kurth Legal Note—How the GDPR Regulates AI (March 2020), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf.

CIPL AI Second Report—Hard Issues and Practical Solutions (February 2020), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_second_report_-_artificial_intelligence_and_data_protection_-_hard_issues_and_practical_solutions__27_february_2020_.pdf.

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?

CIPL has decided to skip this question

Mission one: Unlocking the value of data across the economy

Data is an incredibly valuable resource for businesses and other organizations, helping them to deliver better services and operations for their users and beneficiaries. However, there is increasing evidence to suggest that the full value of data is not being realised because vital information is not getting to where it needs to be.

Our first mission is to create an environment where data is appropriately usable, accessible and available across the economy – fuelling growth in organizations large and small. We will create a clearer policy framework to identify where greater data access and availability across and with the economy can and should support growth and innovation, in what form, and what government's role should be, in the UK and globally.

Data availability: For data to have the most effective impact, it needs to be appropriately accessible, mobile and re-usable. That means encouraging better coordination, access to and sharing of data of appropriate quality

between organizations in the public sector, private sector and third sector, and ensuring appropriate protections for the flow of data internationally.

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) (https://onsdigital.github.io/dp-classification-tools/standard-industrial-classification/ONS_SIC_hierarchy_view.html) codes.

- Charity or Non-Profit
- Public Sector/Central or Local Government, including Defence
- Financial and Insurance Activities
- Information and Communication
- Professional, Scientific and Technical Activities
- Accommodation and Food Service Activities
- Administrative and Support Service Activities
- Agriculture, Forestry and Fishing
- Arts, Entertainment and Recreation
- Construction
- Education
- Electricity and Gas supply
- Human Health and Social Work Activities
- Manufacturing
- Mining and Quarrying
- Real Estate Activities
- Transportation and Storage
- Water Supply and Waste Management
- Wholesale and Retail Trade
- Other (please specify – all of the above):

Please give any further details about your selections here:

CIPL does not have any data to support a ranking of these sectors. However, we believe that appropriate and accountable data sharing between and among both public and private sector organizations has the potential to benefit all sectors and the public.

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

The central government has a crucial role in articulating, promoting or supporting appropriate policy and legal frameworks to improve access to data for all relevant economic actors in all sectors. Constructive engagement with such actors is also crucial while central government undertakes its leadership role, as well as promoting constructive engagement on an ongoing basis and with other regulators. Trust in the data economy and society should be promoted and facilitated through accountability and data sharing frameworks that protect data but also enable access and responsible uses of data based on the associated risks to individuals. Such data sharing frameworks could cover for instance data governance, data sharing processes, due diligence processes, specific tech developments (e.g. common APIs, data sharing processes, etc.), as well as both personal and non-personal data. Due consideration should be given to when voluntary and mandatory data sharing is more appropriate and that certain data cannot be shared due to confidentiality and sensitivity issues. Data sharing, in particular in the public sector, is important to drive efficiencies in governance, data use for good and to improve public services and evidence policy making. As the government and public sector are also subject

to data protection obligations, the UK central government should be extra cautious in holding the public sector accountable to the UK data protection standards. Additional education and capacity-building initiatives would be welcome on this front.

Data sharing is needed not only within the UK, but also across borders, in particular given that many of the organizations involved in developing technological solutions have a global reach. Part of the central government's work to promote data sharing will therefore be also educating governments and international bodies on the importance of data sharing and access to open data, as well as the problems that initiatives such as data localization can cause to the digital economy.

Also, the materials by Professor Christopher Hodges and CIPL on modern approaches to effective regulation, including in data protection, (addressed above in Q.1) are directly relevant to the question of how the Central Government can enable better access across the wider economy.

Finally, government should proactively incentivize accountable and responsible organizations in enabling them to engage in data sharing initiatives. There should be a positive "incentive" for those that demonstrate their accountability and responsibility in data management (including through external certifications), such as allowing these organizations to participate in public procurement, or data sharing initiatives, allowing for mitigation in enforcement, showcasing the best practices and best-in-class organizations and even providing economic incentives.

CIPL has written a memorandum to DCMS following a meeting with CIPL members on data privacy within the UK National Data Strategy, where we highlighted the points above and other related points discussed during this meeting – for reference, the memorandum is available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_key_points_and_messages_cipl-dcms_7_oct_2020_roundtable__26_nov_2020_.pdf. See also answer to Q19.

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

CIPL believes that the government should take on a leadership role in data sharing by modeling effective and accountable data sharing initiatives between governmental bodies as a first step and by developing effective accountability frameworks for receiving and using private sector data for the public good. Government should also proactively incentivize good behaviors, accountable and responsible data sharing practices and actors.

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

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

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

Please explain your answer here. If applicable, please indicate what you think this role should be.

CIPL has recently submitted comments in the EU Data Strategy consultation which are directly applicable to the UK strategy and in particular its "data foundations" and "data availability" components as well—CIPL Response to the EU Commission's Consultation on a European Strategy for Data (May 2020), available at

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_the_eu_commissions_consultation_on_a_european_strategy_for_data__29_may_2020_.pdf.

Consistent with the points we made in that consultation, the following points describe key features of the government's role in developing a sensible UK data access and sharing framework in line with the goals of the UK Data Strategy:

1. The UK government's role should be to create a light touch, agile and iterative governance framework for data sharing, access and use. CIPL believes that a framework based on demonstrable and enforceable organizational accountability and its essential elements is critical to enabling this such sharing, access and use, while also preserving trust in data use and sharing. It can resolve several existing challenges for different forms of data sharing relationships (i.e. B2B, B2G, G2B, G2G). It would also address an apparent lack of trust between market players in sharing data and reluctance to open up data for research, data for good and beneficial purposes.
2. The data strategy should call for the UK ICO to work with organizations to develop a framework for accountable data sharing that can work with the UK Data Protection Act of 2018 and that is in line with the ICO's recently released Accountability Framework. Developing this data sharing framework should include exploring how to encourage organizations to adopt accountable best practices and safeguards to ensure responsible data sharing. In contexts where individual choice to share data might be appropriate and practicable, the concept of personal data spaces should also be explored.
3. An important first step in the creation of an accountable data sharing framework involves resolving key challenges of the UK Data Protection Act 2018, which may create some reticence in both large organizations and SMEs to engage in data sharing, impose barriers to the responsible flows of data between organizations, and provide legal uncertainty for organizations. This includes finalizing the UK Data Protection Act 2018 certification and code of conduct frameworks, providing a completed DPA international transfer toolkit, providing a consistent definition and interpretation of anonymous data, clarifying the legal regime applicable to pseudonymous data, promoting progressive interpretations of some key data protection concepts, such as legal bases for processing (e.g. legitimate interest and public interest) and clarifying how the legal basis can be used for data sharing, using and sharing data for "not incompatible" purposes, exemptions related to processing for research purposes, and the role of risk assessments that include assessments of the benefits of processing, reticence risk as well as risks to individuals.
4. The UK strategy for data, including proposed legislation and any governance framework for accountable data sharing must incorporate a risk-based approach. This means an approach based on risk assessment with rules and requirements calibrated depending on the level of risk involved. Such an approach would build on the existing experience under the GDPR and UK Data Protection Act 2018 where many organizations already conduct data protection impact assessments (DPIA) for high risk processing, including some data sharing purposes. Practically, this means that for each data sharing project or initiative, an organization must complete a risk assessment to understand the risks and harms to individuals involved, as well as the benefits and progress that the envisaged data sharing would bring to individuals and wider society. This could form part of a DPIA for high risk processing or be carried out through a specific data sharing impact assessment where appropriate. Assessment and balancing of different human rights may also be relevant (e.g. for some data sharing to fight the COVID-19 crisis, the right to privacy and data protection had to be balanced with the right to life and health). The assessment must also consider reticence risk, or the opportunity cost of not engaging in the data sharing. All of these factors are integral to the risk assessment formula. The output of this formula then facilitates risk-based calibration of rules and obligations to ensure high risk data sharing receives higher levels of attention.
5. A UK data strategy must be developed with an eye on global interoperability and collaboration if the UK wants to create a truly attractive policy environment for its data economy. Long-standing UK/EU rules on international data transfers have ensured that European (now UK) protections follow the data regardless of where it travels globally. The UK strategy for data should be based on a similar model, although there is significant need as well as scope to improve and streamline the EU data transfer mechanisms, as further

addressed in Q18. Any type of data residency requirement or obligation to store data in the UK would raise several challenges and hinder the ability of UK organizations to innovate. Equally, the UK should continue to be vocal in opposing data localization trends in other countries.

6. The UK strategy for data should promote and incentivize voluntary sharing arrangements and understand their sufficiency and effectiveness for accountable data sharing before considering compulsory data sharing schemes.

7. An innovative and future oriented UK data strategy should provide for innovative regulatory oversight that includes regulatory sandboxes and data review boards. In this context, the regulatory sandbox concept already in use by the UK ICO would provide a safe space for testing innovative forms and methods for data use and sharing under the supervision of a data protection authority or other appropriate regulator. Data review boards may also serve as an agile oversight tool to help organizations make responsible decisions about data use and sharing, and to demonstrate their commitment to ethical decision-making to regulators, individuals and society. They provide an opportunity to receive expert and independent perspectives on proposed data use and sharing initiatives detached from commercial interests.

8. Consistent with nudge theory of behavioral economics, government must put in place "incentives" to encourage and reward those organizations that are implementing and are able to demonstrate accountability in their data use and management (as mentioned above). This also includes ensuring regulators also adopt the same outlook of encouraging, rewarding and showcasing best-in-class, as opposed to resorting to hard enforcement straight away.

Please refer to the following CIPL Paper: Regulatory Sandboxes in Data Protection - Constructive Engagement and Innovative Regulation in Practice (March 8, 2019), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_regulatory_sandboxes_in_data_protection_-_constructive_engagement_and_innovative_regulation_in_practice__8_march_2019_.pdf.

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?

To address the particular challenges of SMEs, it would be particularly helpful to encourage and undertake the development and implementation of codes of conduct and certifications (as envisioned by the GDPR/UK Data Protection Act 2018), and especially programmatic certifications that certify an entire data protection management program, both for domestic compliance and for cross-border transfer purposes. These could also cover accountable data sharing issues. For global interoperability with CBPR and other global schemes (see below), it is essential that there be programmatic certifications and codes of conduct, not just certifications or codes that cover only specific processing operations or products.

As immediate steps, the central government should set up a simple, pragmatic and scalable certification framework and promote certifications and their benefits among UK businesses, including SMEs. The UK should also develop this framework with an eye to similar existing global schemes to ensure interoperability, such as certifications provided by the International Organization for Standardization (ISO), the APEC Cross-Border Privacy Rules (CBPR) System, binding corporate rules (BCR) and others.

The UK should also further unlock the potential of BCR as an international data transfers tool. For instance, organizations with approved BCR should be able to share data among themselves without having to rely on any specific transfer tool as they already comply with the highest data protection standards. The same reasoning should apply to transfers between companies with approved BCR and certified companies or companies adhering to a code of conduct. (See also response to Q18.)

See for reference the CIPL Certifications Paper—Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms (April 2017), available at

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf.

The Smart Data Review (https://www.gov.uk/government/consultations/smart-data-putting-consumers-in-control-of-their-data-and-enabling-innovation) in 2019 consulted on ways to make evolving schemes more coordinated across banking, finance, telecoms and energy. The focus of Smart Data is citizens asking their providers to share information about them with third parties.

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?

See answers to Questions 7 and 8.

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

Building on our status as a world leader in technological innovation and our robust data protection standards, we will maintain a data regime that supports the future objectives of the UK outside of the EU and promotes growth and innovation while maintaining public trust. This regime will not be overly burdensome for the average company, nor will it be unnecessarily complex or vague; it will help innovators and entrepreneurs use data legitimately to build and expand their businesses, without undue regulatory uncertainty or risk at both the domestic and international levels.

To encourage the widespread uptake of digital technologies, we will also work with regulators to provide advice and support to small- and medium-sized businesses to help them expand online, and develop sector specific guidance and co-regulatory tools to accelerate digitisation across the UK economy.

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

To remain fit for purpose in the digital economy and society in which the importance of data will only increase, the UK's data protection framework should be interpreted and applied consistently with its inherent principle-based, outcome-based and risk-based approach of the UK Data Protection Act 2018. If interpreted in light of these core concepts, the UK's data protection framework will be a solid foundation for building effective protection and trust for individuals while enabling the digital economy, including at time of crises. CIPL has written several white papers in the context of the GDPR that outline both existing challenges presented by the GDPR's provisions in the context of the modern data economy, as well as the benefits the GDPR delivers in that context, particularly when interpreted flexibly and in light of the principle-based, outcome-based and risk-based approach. The arguments presented in these papers are equally applicable to the UK Data Protection Act 2018. These papers are:

CIPL Response to the EU Commission's Public Consultation on the Evaluation of the GDPR (April 2020), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_eu_commission_consultation_on_gdpr_evaluation__28_april_2020_.pdf.

CIPL GDPR Stocktaking Report - GDPR One Year In - Practitioners Take Stock of the Benefits and Challenges (May 2019), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_report_on_gdpr_one_year_in_-_practitioners_take_stock_of_the_benefits_and_challenges.pdf.

In addition, UK should take full margin of maneuver allowed under GDPR to put forward more progressive interpretation of the law, tweak areas that do not seem to work well, and propose additional rules where possible. The Information Commissioners' Office should be encouraged to continue to be a leading data protection authority and take a pragmatic, risk-based and practical approach, based on constructive engagement

with regulated entities. Finally, UK must take full advantage of progressive, but under-used elements of the GDPR, such as (i) the risk-based approach to calibrate legal requirements and compliance, (ii) accountability and (iii) codes and certifications. This will enable a lighter, more forward-thinking and future-proof regime that is based on co-regulatory frameworks and more adaptable to the digital society and economy.

UK government must also consider how the data protection regime fits with other areas of digital law and policy, including consumer, competition, AI, online harm, platform/content and cybersecurity. Many organizations are struggling to address all of these compliance requirements in a coherent way and follow disparaging developments. This is true for large organizations, and even more for SMEs. It is essential that there is no conflict, nor overlap with different regulatory areas—from policy, law and regulatory oversight perspectives.

More specifically, there is a real problem in how organizations comply with the UK Data Protection Act 2018 and the UK implementing rules and guidance under old ePrivacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)). The EU legislative process of the ePrivacy Regulation, which is supposed to replace the ePrivacy Directive, has also exposed serious concerns and doubts about the newly proposed rules. With UK not being bound by the eventual new ePrivacy Regulation, this may be an opportunity for the UK to re-think if and how to re-align the provisions of the UK Data Protection Act 2018 with the existing Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). This will be much welcome and necessary in order to ensure legal certainty, proper functioning of the PECR rules work with the new UK Data Protection Act 2018 and that these rules are updated to the realities of modern data processing. This may mean amending or incorporating some of the still valid provisions of PECR.

In addition to ensuring that the data protection framework reflected in the UK Data Protection Act 2018 is properly and effectively realized and implement per the above, it is also important to enable more broadly a modern regulatory framework along the lines described in the work of Professor Chris Hodges and CIPL's white paper on "Regulating for Results" discussed in response to Q.1 above. Please, refer to some answers we gave to questions above about smart regulation and reticence risks.

In section 7.1.2 we lay out the functions of the Centre for Data Ethics and Innovation (CDEI), set up in 2018 to advise the Government on the use of data-driven technologies and AI.

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.

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

Please explain your answer here:

CIPL strongly supports the proposed functions and role of the CDEI as set forth in the National Data Strategy. CIPL has been a long-standing proponent of increasing public trust in the data economy through organizational accountability, digital responsibility and transparency, both in the public and private sectors, and in relation to all aspects of data processing and data-driven technologies, including in the context of AI and data sharing. We have commented extensively on defining a regulatory path for AI in the EU. Our comments are equally relevant in the UK. In the EU, we have argued for a layered approach to regulating AI in the following way:

(1) A minimal, principles-based, outcome-based and risk-based approach, relying primarily on existing laws and standards

(2) Risk-based, demonstrable and verifiable accountability measures and practices of organizations
(3) Smart regulation and oversight based on co-regulatory instruments (e.g. codes of conduct and certifications), regulatory sandboxes and regulatory hubs.

We believe that the CDEI is well positioned to substantially contribute and enable this approach to regulating AI, data-driven technologies and all modern data-processing activities. Equally, we believe that the UK data strategy more generally is substantially in alignment with this approach and to that extent we fully support it.

However, it is important to ensure that the role of CDEI is properly scoped and does not overlap with the UK ICO's remit, especially their thought-leadership and guidance work. UK ICO has been a leading tech regulator in the UK and has much business, technology and regulatory acumen to increase its role, remit and importance. It is important that CDEI has a complimentary role to the ICO and other regulators, supporting their work, but with a separate and different remit—perhaps more like a governmental think-tank. Finally, CDEI has to be fully resourced and more visible in national debates about data and technology role in our digital society and economy.

Please refer to the following CIPL white papers on this topic:

CIPL Response to the EU Commission's AI White Paper (June 2020), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_eu_consultation_on_ai_white_paper__11_june_2020_.pdf.

CIPL/Hunton Andrews Kurth Legal Note - How the GDPR Regulates AI (March 2020), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf.

CIPL AI Second Report - Hard Issues and Practical Solutions (February 2020), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_second_report_-_artificial_intelligence_and_data_protection_-_hard_issues_and_practical_solutions__27_february_2020_.pdf.

CIPL AI First Report - Artificial Intelligence and Data Protection in Tension (October 2018), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_first_ai_report_-_ai_and_data_protection_in_tension__2_.pdf.

CIPL Submission to the Review of Artificial Intelligence and Public Standards by the UK's Committee on Standards in Public Life (July 2019), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_cspl_submission_july_2019.pdf.

CIPL Response to ICDPPC Declaration on Ethics and Data Protection in Artificial Intelligence (January 2019), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_icdppc_declaration_on_ethics_and_data_protection_in_artificial_intelligence.pdf.

Q11a. How would a change to statutory status support the CDEI to deliver its remit?

CIPL has decided to skip this question

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

There is massive untapped potential in the way the government uses data. We will implement major and radical changes in the way that the government uses data to drive innovation and productivity across the UK. In doing so,

we will improve the delivery of public services, as well as our ability to measure the impact of policies and programmes, and to ensure resources are used effectively.

To succeed, we need a whole-government approach led by a Government Chief Data Officer from the centre in strong partnership with organizations. We need to transform the way data is collected, managed, used and shared across government, including with the wider public sector, and create joined-up and interoperable data infrastructure. We need the right skills and leadership to understand and unlock the potential of data – and we need to do so in a way that both incentivises organizations to do the right thing, as well as build in the right controls to drive standardisation, consistency and appropriate data use.

The government is going to set an ambitious package of work in this space and wants to understand where we can have the biggest impact.

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.

CIPL supports the goals of "Mission three" and believes that each of the specific areas of work identified above are equally important as well as interdependent, as improvement and success in one area depends on improvement and success in the others.

Q13. The Data Standards Authority is working with a range of public sector and external organizations to create a pipeline of data standards and standard practices that should be adopted.

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

CIPL has decided to skip this question

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

In the UK, the government already imposes safeguards and enforcement regimes to ensure that our data is handled responsibly. But we will also take a greater responsibility for ensuring that data is sufficiently protected when in transit, or when stored in external data centres.

The government will determine the scale and nature of risks and the appropriate response, accounting for emerging trends in the market landscape. We will also determine whether current arrangements for managing data security risks are sufficient to protect the UK from threats that counter our missions for data to be a force for good. And we will consider the sustainability of data use, exploring inefficiencies in stored and processed data, and other carbon-inefficient processes.

The infrastructure on which data relies is the virtual or physical data infrastructure, systems and services that store, process and transfer data. This includes data centres (that provide the physical space to store data), peering and transit infrastructure (that enable the exchange of data), and cloud computing that provides virtualised computing resources (for example servers, software, databases, data analytics) that are accessed remotely.

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?

CIPL has decided to skip this question

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?

One way is to address this issue is through privacy and data security codes of conduct and certifications. They can serve as effective due diligence tools by helping to identify accountable and responsible data infrastructure services, including data processors and cloud providers that are adhering to such codes or have received a relevant certification. Thus, we urge that relevant codes and certifications, envisioned by the GDPR/UK Data Protection Act 2018, are developed and made available as a matter of priority.

Q15. Demand for external data storage and processing services is growing. In order to maintain high standards of security and resilience for the infrastructure on which data use relies, what should be the respective roles of government, data service providers, their supply chain and their clients?

CIPL has decided to skip this question

Q16. What are the most important risk factors in managing the security and resilience of the infrastructure on which data use relies?

For example, the physical security of sites, the geographic location where data is stored, the diversity and actors in the market and supply chains, or other factors.

CIPL has decided to skip this question

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

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

Please explain your answer here. If applicable, please indicate how the government can effectively ensure that data does not negatively contribute to carbon usage.

CIPL has decided to skip this question

Mission five: Championing the international flow of data

In our hyper-connected world, the ability to exchange data securely across borders is essential.

As the UK leaves the EU, we have the opportunity to develop a new UK capability that delivers new and innovative mechanisms for international data transfers.

Using our reputation as a world leader in digital, a champion of free trade and the rules-based international system, and an engaged, rule-abiding member of the global community, we will build trust in data's use, creating the regimes, approaches and tools to ensure personal data is appropriately safeguarded as it moves across borders. We will also facilitate cross-border data flows by removing unnecessary barriers to international data transfers that promote growth and innovation. And we will seek to promote data standards, data interoperability, and UK values internationally.

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

CIPL recently participated in a call with DCMS to provide input into the above question and related issues and has summarized its input and key messages in a memorandum entitled "Key Issues and Questions Concerning International Data Transfers", which we have shared with DCMS.

This memorandum is also available here: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_key_points_and_messages__cipl-dcms_september_24_roudtable__9_nov_2020_.pdf.

In that memorandum, CIPL describes the ways in which the UK can effectively implement, improve and streamline the various GDPR/UK Data Protection Act 2018 transfer mechanisms—Binding Corporate Rules, Standard Contractual Clauses, codes of conduct and certifications, make them interoperable with global counterpart transfer mechanisms such as CBPR, and how the UK could otherwise participate in the development of global solutions to the governance of cross-border data flows both through and outside of the EU and UK based transfer mechanisms.

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.

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?

Country-wide (or even sectoral) adequacy findings, are of great value to industry. Adequacy findings should be prioritized through the lens of greatest impact on the UK economy (i.e. countries with the greatest volume of cross-border data transfers from the UK) and through the lens of the level of complexity of the analysis (i.e. some countries may be easier and faster to assess as they either have or had EU adequacy findings or have better known or trusted legal regimes). We have addressed issues related to adequacy in the above referenced memorandum to DCMS in Q18.