29 May 2020

Centre for Information Policy Leadership's Response to the EU Commission's Consultation on a European Strategy for Data

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to the European Commission's consultation on its European Strategy for Data.[2] Recent events – and in particular the need for data sharing within the context of the COVID-19 pandemic – have only 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 AI, making data sharing and ensuring the availability of data a critical component of the EU's AI strategy. CIPL appreciates the Commission's effort to create a strategy that aims to increase the use of, and demand for, data and data-enabled products and services throughout the European Digital Single Market. CIPL further commends the Commission for considering the strategy through a holistic lens and addressing aspects such as the availability of data, opportunities to use data for social and economic good, market power and data for SMEs, interoperability, data infrastructure, digital literacy and data protection and cybersecurity. Given the broad nature of the strategy, CIPL's comments below focus mainly on data protection aspects, while providing more general feedback on other areas of the consultation. In reading CIPL's comments, it is important to keep in mind that the EU General Data Protection Regulation[3] already provides a data protection framework for the sharing of personal data between organisations. Article 4(2) of the GDPR states that the processing of personal data includes "[…] disclosure by transmission, dissemination or otherwise making available […]."

CIPL's Key Messages

1. CIPL welcomes the Commission's approach to create a **light touch, agile and iterative governance framework** for data access and use. CIPL believes that a framework based on demonstrable and enforceable organisational accountability and its essential elements is critical to enabling this approach, while preserving trust in data use and sharing. Accountability also enables the transformation of organisations in a way that fits well with a data-agile economy and enables vivid ecosystems to develop as envisioned by the data strategy.

2. The data strategy should call for the European Data Protection Board (EDPB) and national Data Protection Authorities (DPAs) to **work with organisations to develop a framework for accountable data sharing that can work with the GDPR**. Developing this framework should include exploring how to incentivise organisations 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 GDPR challenges**, which create some reticence in both large organisations and small and medium-sized enterprises (SMEs) to engage in data sharing, impose barriers to the responsible flows of data between organisations, and provide legal uncertainty for organisations. This includes finalising the GDPR certification and code of conduct frameworks, providing a completed GDPR 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), 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. To ensure the success of a common data space, Europe needs to ensure a common framework. Addressing issues of **harmonisation at national and sectoral level** is critical in this regard. Establishing regulatory hubs can assist in reconciling any conflicts or diverging approaches of regulators.

5. Creating a data sharing **framework based on accountability** 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.

6. The European 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 where many organisations 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 organisation 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.

7. A European data space must be developed with an eye on **global interoperability and collaboration** if Europe wants to create a truly attractive policy environment for its data economy. Long-standing EU rules on international data transfers have ensured that European protections follow the data regardless of where it travels globally. The European strategy for data should be based on a similar model. Any type of data residency requirement or obligation to store data in Europe would raise several challenges and hinder the ability of European organisations to innovate. Equally, the EU should continue to be vocal in opposing data localisation trends in other countries.

8. The European strategy for data should promote and **incentivise voluntary sharing arrangements** and understand their sufficiency and effectiveness for accountable data sharing before considering compulsory data sharing schemes.

9. An innovative and future oriented EU data strategy should provide for **innovative regulatory oversight that includes regulatory sandboxes and data review boards.** In this context, the

regulatory sandbox concept would provide a safe space for testing innovative forms and methods for data use and sharing under the supervision of a DPA or other appropriate regulator. Data review boards may also serve as an agile oversight tool to help organisations 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.

10. In creating common European data spaces, the data strategy should make clear that any **sectoral frameworks should be in alignment with the proposed cross-sectoral horizontal framework** and should based on organisational accountability.

Comments on the Strategy

Section 2: What is at Stake?

The European Commission notes that in order to ensure Europe's success in the data economy, it must find its own European way of balancing the flow and wide use of data with preserving high privacy, security, safety and ethical standards. CIPL welcomes Europe's ambition to compete with other bustling data markets, including the United States and China. At the same time, it is important to keep in mind the global nature of data innovation and trade as well as Europe's participation and role in the global digital landscape in designing the data strategy. Moreover, as Europe continues to foster global relationships with foreign economies, it must find ways to ensure that the European approach does not lead to an insular data society which could undermine the EU's ability to become a leader in AI and otherwise limit the value of data and methods to share data for European society as well as the wider world.

The Commission outlines various steps it has already taken to shape the data economy of the future and mentions how the GDPR has created a solid framework for digital trust. In forming any European strategy for data, it is crucial that the drafters keep this framework (as well as other European instruments, directives and regulations) in mind to avoid duplicative and potentially conflicting standards, rules and guidelines. The GDPR provides a comprehensive framework for the handling of personal data and regulates, in many ways, how data can be used and shared. CIPL recently provided input to the Commission's consultation on the evaluation of the GDPR,[4] highlighting the tangible benefits of the GDPR as well as the challenges that need to be addressed to make the GDPR an enabler of the European data economy.

In particular, the data strategy should consider how some long-standing core principles of data protection (such as purpose limitation, legal bases for processing, data minimisation, etc.) and the lack of clear allocation of responsibilities in controller-to-controller relationships may stifle important data sharing practices. In this regard, CIPL recommends that the data strategy should call for the EDPB and national DPAs to work with organisations to develop a framework for accountable data sharing that can work with the GDPR. Ideally, such a framework should avoid an approach that adds friction by making data sharing systematically dependent on choices made by individuals. Otherwise, it may actually defeat the data sharing purpose by making it overly burdensome for organisations and laborious for individuals who may struggle to intervene frequently enough to support this approach at the necessary scale. Rather, DPAs and the EU Commission should incentivise organisations adopting accountable best practices and safeguards to ensure responsible data sharing. However, in contexts where individual choice to share data might be appropriate and practicable it may be possible to also

create personal data spaces where people could agree in advance with whom and for what purposes they would like to share their data. All of these options should be further explored with the aim of creating a framework that is human centric, where appropriate, on the one hand but recognises the need for data sharing for wider societal benefits on the other. The EDPB and DPAs have a critical role to play in raising awareness among organisations of the importance of data sharing and debunking misconceptions that sharing data with third parties is inherently contrary to data protection, always poses high risks and should be avoided. In clarifying these issues, DPAs should proactively enable responsible data sharing that can yield benefits for all if undertaken within appropriate accountability frameworks (see further discussion below under Section 5).

An important first step in the creation of an accountable data sharing framework involves resolving key GDPR challenges, which create some reticence in both large organisations and small and medium-sized enterprises (SMEs) to engage in data sharing, impose barriers to the responsible flows of data between organisations, and provide legal uncertainty for organisations:

- **Certifications and Codes of Conduct**: The European Commission, the EDPB and the DPAs should finalise the GDPR certification and code of conduct frameworks promptly to enable data sharing co-regulatory frameworks that integrate data protection and security.[5] To date, not a single GDPR certification or code of conduct has been officially approved, despite the GDPR entering into force over two years ago.

- **Completion of the GDPR International Data Transfer Toolkit**: In addition to the development of certifications and codes of conduct, which can serve as data transfer tools and facilitate the free flow of data, it is imperative that the European Commission, along with the EDPB and DPAs complete the data transfer toolkit provided by the GDPR to facilitate international data sharing initiatives. The need for smooth and undisrupted cross-border data flows to address global issues has been reiterated in the context of the COVID-19 pandemic. For example, IBM and the Weather Channel use data from government bodies globally and the World Health Organization to give over 300 million monthly visitors access to detailed virus tracking.

    - *Standard Contractual Clauses (SCCs)*: There is an urgent need for the European Commission to finalise the adoption of updated SCCs in line with the GDPR.[6] For instance, to reflect and clarify the relationship with Article 28 processor obligations, to consider the territorial scope of the GDPR, to enable SCCs for new transfer scenarios such as processor-to-processor transfers, etc.

    - *Binding Corporate Rules (BCR)***:** The GDPR enables the use of BCR to legitimise transfers of data between a group of undertakings or group of enterprises engaged in a joint economic activity. However, this enabling provision has not been implemented nor incentivised by the Commission, the EDPB and the DPAs. There is every reason to enable data sharing between responsible companies, where both of them have put in place and obtained regulatory approvals for their internal privacy management programs (i.e. BCR).

    - *Review of Adequacy Decisions*: The Commission should also review existing adequacy decisions without delay and continue negotiations with nations seeking adequacy for the first time.

Importantly, a European strategy for data cannot be viewed from the perspective of filtering data into Europe alone. Many foreign data trading partners will expect an exchange of data with Europe and global data driven initiatives that Europe is a part of will inevitably involve data sharing with other countries. Data must be able to flow freely from the EU to other nations in line with a full and complete set of international transfer tools as envisioned and provided by the GDPR. In this regard, CIPL agrees with the Commission's view that a European data space should ensure there is an open, but assertive approach to international data flows, based on European values. The long-standing approach of Europe's data protection framework under both Directive 95/46/EC[7] and subsequently under the GDPR has been to ensure that European protections follow the data regardless of where it travels. To the extent data sharing involves personal data, the European strategy for data must necessarily work with the GDPR transfer requirements. Thus, for example, a country that is deemed adequate for data transfer purposes generally will also be adequate for data sharing purposes with respect to personal data. By completing the GDPR's transfer toolkit, any data that is shared from Europe to other nations will ensure that European values attach and are transferred along with the data.

- **Anonymisation and Pseudonymisation**: As our digital society increasingly requires that data moves between different stakeholders (businesses, public authorities, civil society bodies, NGOs and academic institutions), the role of anonymisation and pseudonymisation becomes more and more relevant. Such forms of data can reduce the risks associated with using and sharing personal data and can facilitate innovative uses of data that might otherwise not be permitted.

    - *Anonymised Data***:** The strategy notes that use of aggregated and anonymised social media data can be an effective way of complementing the reports of general practitioners in case of an epidemic. We have recently seen real life discussions related to this very issue as countries explore how to combat the COVID-19 pandemic, including through community mobility reports and contact tracing apps. Yet, there exists a lack of consistency among DPAs on the interpretation of anonymisation and how to achieve it.[8] CIPL recommends that the data strategy call for a consistent definition and interpretation of anonymous data. Such consistency is key to building and maintaining the trust of individuals in the data economy and the benefits it can bring to them as well as wider society. The standard put forward by the US Federal Trade Commission in a 2012 privacy report: reasonable de-identification coupled with contractual and legal safeguards against inappropriate re-identification, could provide an appropriate benchmark.[9] This standard accounts for the fact that anonymisation is not a static exercise but one in which the anonymisation process depends on context and reasonably available de-identification techniques.

    - *Pseudonymous Data*: Under the GDPR, pseudonymous data qualifies as personal data. Yet, such data can no longer be attributed to a specific data subject without the use of additional information and its processing poses very little risks to individuals. In line with the risk-based approach of the GDPR, organisations should be allowed to process pseudonymous data under an adapted regime that does not impose the full-fledged requirements of the GDPR (provided relevant technical and organisational risk mitigation measures and safeguards have been implemented). CIPL recommends that

the data strategy call for clarification around the legal regime applicable to pseudonymous data.

- **Progressive Interpretation of Key Data Protection Concepts**: The GDPR is a principles-based law designed to be future proof and adaptable to new data uses and ways of sharing data. To ensure the success of the European data strategy in enabling data sharing to thrive, it is imperative that the Commission calls for progressive interpretation of key data protection concepts by the EDPB and DPAs, both generally and as they relate to data sharing specifically.

    - *Legal Basis for Processing*: The GDPR provides six legal bases for processing data, none of which are privileged over the other. Yet, there is perception that DPAs, lawmakers and policymakers in the EU place a strong emphasis on consent as a more protective legal basis based on the questionable belief that consent inherently empowers individuals. In the data sharing context, while consent has a role to play in certain circumstances, many forms of data sharing are more suited to other legal processing grounds such as legitimate interest or public interest. For instance, the COVID-19 crisis has brought the significance of public interest into focus as an enabler of the use of personal data for social good. The EDPB recently clarified that, under the GDPR, private entities involved in the fight against COVID-19 may rely on the public interest derogation for cross-border transfers of data used for research.[10] DPAs have a responsibility to support broader, more innovative and flexible interpretations of all legal bases for processing. This is critically important as data sharing is likely to make use of the full range of processing grounds. For instance, consent may be appropriate in the context of data altruism; it may be contractually necessary to share data in the context of data service delivery to individuals; public and vital interest are key to enabling data sharing to respond to matters of important public policy and emergencies, as well as enabling data for social good; legitimate interest is essential for data sharing in the fight against fraud and to ensure network and system security; and legal obligations to share data exist in different regulatory fields, such as for anti-money laundering purposes.

    - *Using Data for "Not Incompatible" Purposes*: There is a need for a broader interpretation of what constitutes a "not incompatible" purpose. Organisations should be able to share personal data for new and beneficial purposes even when such purposes are different from the original purpose for which the data was collected and were not envisaged at the time of collection provided that the organisation sharing the data adopts all appropriate accountability measures, including risk assessments for the new purpose, and ensures relevant safeguards. Ensuring the correct interpretation of a "not incompatible" purpose is vital to enabling beneficial uses of data for good as well as data processing that brings value to individuals and society. Re-use of data for compatible purposes is integral to many examples cited by the European Commission, including to combat emergencies such as natural disasters, to tackle climate change and fight against crime and for the development and training of artificial intelligence. In this regard, it will be important to create new protocols to allow for further processing of personal data, including sensitive data, in more instances than has been the case to date. In many cases, these new uses may involve using anonymous or pseudonymous data, which will enable risks and harms to be

mitigated appropriately. Such new protocols will also need to be created where personal data (as opposed to anonymous or pseudonymous data) has to be used, as the objectives of processing may not be able to be fulfilled by the use of anonymous data.

- *Exemptions for Research*: Data sharing is essential for enabling advancements in research. However, organisations often report reticence and caution when embarking on data-sharing projects, for fear of breaching applicable data protection laws or due to a lack of clarity on what regulators and the public may expect. Many report the need for a broader interpretation of data protection provisions that enable the use of personal data for statistical and research purposes. DPAs have a vital role to play in ensuring the interpretation of the scientific research exemption under Article 89 is made more broadly available to private sector organisations. DPAs should confirm that when data protection law provides that scientific research is exempted from some of the legal requirements, this exemption extends to all organisations for data analytics, research and algorithmic training purposes.

- **Role of Risk Assessments**: The GDPR embeds the risk–based approach to allow for consideration of risks and harms to individuals and to calibrate compliance based on these risks and harms. However, there is a general sense that the risk-based approach is often neglected in the official guidance from DPAs and the EDPB. Yet, it is this very approach that would allow the GDPR to stay future proof and continue to adapt to new ways of using and sharing data, especially where they are bringing real benefits for individuals and society at large (provided risks and harms are not severe or likely, or have been mitigated). To ensure that the European strategy for data, including proposed legislation and any governance framework for accountable data sharing remains future proof and flexible, it is critical that the Commission articulate the risk-based approach to data sharing in the strategy. 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 where many organisations already conduct DPIAs for high risk processing, including some data sharing purposes. Practically, this means that for each data sharing project or initiative, an organisation 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.

Section 3: The Vision

CIPL agrees with the Commission that businesses and the public sector in the EU can be empowered through the use of data to make better decisions, especially within the context of data for social and economic good. CIPL believes that it is possible to create a single European data space that facilitates access to high-quality data in line with EU law through the creation of an accountable and enforceable data sharing framework. CIPL agrees with the Commission's vision that a European data space must be built on common European rules and enforcement mechanisms that ensure data flows within the EU and across sectors, respects European rules and values, provides clear and trustworthy data governance mechanisms and provides an assertive approach to international data flows. These factors are of critical importance and must be considered as the EU works on a framework for accountable data sharing.

Critically, a European data space must be developed with an eye on global interoperability and collaboration if Europe wants to create a truly attractive policy environment for its data economy. As mentioned above, long-standing EU rules on international data transfers have ensured that European protections follow the data regardless of where it travels. To the extent data sharing involves personal data, the European strategy for data must necessarily work with the GDPR transfer requirements. Any type of data residency requirement or obligation to store data in Europe would raise several challenges and hinder the ability of European organisations to innovate. Equally, the EU should continue to be vocal in opposing data localisation trends in other countries.

Section 4: The Problems

The European Commission has identified several challenges that are holding the EU back from realising its potential in the data economy. CIPL believes these challenges are not insurmountable and can be resolved through engaging on the issues with appropriate stakeholders from different facets of society. CIPL presents its views on each of the problems highlighted below:

- **Fragmentation:** Fragmentation between Member States is a major risk to the vision of a common European data space. In the area of data protection alone, fragmentation between Member States on concepts outlined in the GDPR, including approaches to processing of health and research data or biometric data, have created compliance and operational hurdles as well as a lack of certainty for organisations. To ensure the success of a common data space, Europe needs to ensure a common framework. The Commission has cited several examples where deviation between Member States already exists, including as it relates to data processing for scientific research purposes and on the use of privately held data by government authorities. CIPL stresses the importance of ensuring a uniform approach that works with existing EU rules and, where appropriate and feasible, reconciles conflicts (not only between national approaches, but also between different sectors in cases of cross-sectoral data sharing). This necessarily involves working on harmonisation issues under the GDPR and reducing deviation in implementation of the rules as well as in guidance and interpretation of the requirements from DPAs and other regulators as relevant. Establishing EU level regulatory hubs consisting of different regulators and facilitating their cooperation on any specific conflicts, including through the exchange of views and knowledge, alignment on differing interpretations and participation in joint initiatives can also help avoid fragmented approaches at Member State and sectoral levels. This would be very useful in the AI space, for example, where AI experts from different regulatory bodies could collaborate to prevent

fragmentation while maintaining their independence and competence within their own regulatory field.

- **Availability of data:** The Commission rightly notes that the value of data lies in its use and re-use and that there currently is not enough data available for innovative re-use. With respect to data protection, the GDPR explicitly permits further processing for new, "not incompatible" purposes, while the ePrivacy rules do not permit such further processing. To avoid inconsistent approaches, any future ePrivacy rules should align with the GDPR, especially regarding legal bases for processing and the principle of compatible further processing. CIPL believes that processing based on "compatibility" should be allowed for future uses that are consistent with, can co-exist with, and do not undermine or negate the original purpose – especially where the results of a risk assessment show that the risk to individuals are proportionate with the benefits to society or a specific group of individuals, or other fundamental rights. As mentioned above, re-use of data for compatible purposes is integral to many examples cited by the European Commission, including to combat emergencies such as natural disasters, to tackle climate change and fight against crime and for the development and training of artificial intelligence. In cases where individuals can still be identified in the context of further processing that is not considered a compatible use, it may be appropriate to require consent for data sharing unless certain public policy considerations necessitate otherwise (e.g. law enforcement, emergency situations, etc.)

  The strategy highlights issues relating to various data sharing relationships. CIPL believes that there is value in many forms of data sharing between and among public and private entities and a mechanism for accountable data sharing can provide an appropriate way to address several existing challenges.

  - ***Government to Business***: CIPL supports efforts to improve access to government held datasets. The ability of businesses to access, use and re-use data which has societal value is critical for research and innovation. The Commission also notes that facilitating such access is in line with long-standing EU policy since the adoption of the Directive on the re-use of public sector information.[11] The strategy notes that sensitive data is often unavailable for research purposes in the absence of mechanisms to enable research actions to be undertaken in compliance with data protection rules. While this is an important consideration, there exist various mechanisms to facilitate such data sharing of sensitive data (for all contexts: B2B, B2G, G2B, G2G), including technical measures such as anonymisation and pseudonymisation of datasets, engaging data review boards for new projects, and many different forms of risk assessment and accompanying mitigation measures. Implementing and making use of such mechanisms lies at the heart of an accountable data sharing framework. The strategy should highlight some of these solutions and encourage their use through the broader promotion of accountable data sharing as Governments open up and improve access to data. Public authorities have a critical role to play in the data sharing ecosystem and have an opportunity to lead by example to truly enhance Europe's data economy. They can do this by sharing as much data as possible and adhering to high standards based on accountability in sharing such data. Public procurement processes also afford opportunities to influence and incentivise good data sharing practices throughout the data sharing ecosystem as a whole.

- ***Business to Business***: The Commission highlights various obstacles that have prevented B2B data sharing taking off at scale. Mostly, this is due to a lack of trust between companies, fears around the handling of data once it has been transferred to another entity and possible legal and adverse reputational consequences that may result from sharing the data. For the sender of data, the questions are (1) how far should it go in conducting due diligence on the recipient of data and (2) how can it ensure that the recipient will comply with possible and relevant use restrictions? Conversely, the recipient of data will need to ensure that (1) the data was collected in compliance with the GDPR and (2) that it will be protected and indemnified in cases of inappropriate collection by the sender. CIPL believes that such concerns can be appropriately addressed by enabling an accountable data sharing framework where protections travel with the data and roles and responsibilities of senders and recipients of data can be clarified.

  As our world becomes increasingly digital, companies are beginning to recognise and appreciate that the data they hold alone is not enough to innovate, stay competitive and serve society. A 2018 study by the European Commission on data sharing between companies in Europe demonstrated that companies share and re-use data to enhance their business opportunities and improve internal efficiency. It also revealed that companies not yet engaged in data sharing recognise the benefits of doing so and expressed an intention to start sharing data within the next five years.[12] An important part of facilitating the uptake of data sharing by European organisations is ensuring confidence that their data sharing activities will not be deemed as engaging in prohibited or anti-competitive agreements by antitrust and competition authorities. Thus, CIPL welcomes the current evaluation by the EU Commission DG COMP on the review of the guidelines for horizontal cooperation agreements[13] and stresses the need to adapt these guidelines to account for increasing data sharing practices between companies. In fact, recent examples of data sharing include Google and Apple coming together to work on a privacy-preserving contact tracing initiative to help fight the COVID-19 pandemic.[14] Microsoft and FedEx are also partnering to provide commercial shipping customers with early warnings of delays from weather, traffic and other factors based on data analysis.[15] Not only are the companies able to innovate in new ways through such cooperation and partnership efforts but they are also able to compete with other companies providing similar solutions.

- ***Business to Government***: According to the strategy, there is currently not enough private sector data available for use by the public sector. The benefits of data to Government policy and decision-making are immense. For example, Google is currently making available COVID-19 Community Mobility Reports[16] to aid public health authorities globally in making critical decisions to fight the pandemic. Similarly, Vodafone is providing several European governments with heat maps showing how population movements have changed before and after the imposition of containment measures.[17] Facebook has made available through its Data for Good program high resolution population density maps which the World Bank uses to plan for better COVID-19 resource allocation in Spain.[18] In Germany, Deutsche Telekom has provided aggregated, anonymised data to the Robert Koch Institute (Germany's public health

institute) from its mobile communications network for research into the spread of the coronavirus.[19] It is important to note that while data sharing has increased in response to COVID-19, the data strategy should emphasise the importance of data sharing as part of regular and routine business and not only in crisis contexts. Further, post pandemic we will likely see increased calls for leveraging the power of data and data sharing in all areas of business and government. Many of the services that have been considered essential during the crisis, and/or demanded by customers, were powered by data, provided for free, and often enabled by online advertising. It is safe to say that people – consumers, citizens, employees – will expect the same services in the post-COVID-19 world.

CIPL supports the recommendations of the EU Commission High Level Expert Group on B2G Data Sharing[20] (B2G HLEG) to stimulate B2G data sharing by creating a common framework which will provide legal certainty to both private organisations and government bodies. Again, such a framework (which, as indicated works for all sharing configurations) should be based on organisational accountability – both by the government or public body requesting data and the private organisation sharing data. Accountability within the government and the public sector is just as critical as it is in the private sector. By instilling an approach to sharing data that places responsibility on government bodies and their handling of data they receive, the private sector is likely to share and make available even more data to public authorities. Such an approach will also raise trust levels among individuals that all stakeholders, whether private or public, abide by the same high standards in handling their data.

Furthermore, for B2G data sharing to thrive, the data strategy should acknowledge data collaboration agreements and other data sharing arrangements beyond data philanthropy alone. Collaboration agreements, based on mutually beneficial terms, are one way private organisations and governments can ensure long-term sustainable data sharing. If a public sector body specifically requests private sector data, the private organisation should be entitled to fair compensation for the delivery of the data. Compensation schemes also give businesses the necessary incentives to boost data sharing efforts. Another option for promoting sustainable business to government data sharing could be through European Commission funded data-sharing partnerships. CIPL also supports the funding of pilot B2G data-sharing partnerships in regulatory sandboxes for specific societal challenges.

- ***Government to Government***: CIPL supports data sharing between government bodies. We have already seen the sharing of data for law enforcement and national security and border management purposes between Member States (e.g. The Schengen Information System or Interpol's Secure Information Exchange Network Application). Implementing a data sharing framework based on accountability would provide a platform for further data sharing among national governments and public authorities.

- **Data interoperability and quality**: CIPL agrees that data interoperability and quality are key for the exploitation of the value of data. Data interoperability facilitates data portability

between organisations which can enable more data sharing. However, the strategy highlights that data producers and users have identified several interoperability issues that impede efforts to combine data from different sources. CIPL cautions against the creation of new EU specific formats for data sharing. Many standards on data formats and models already exist and are being developed bottom-up and it is critical that any European efforts on standardisation account for these efforts (e.g. ISO standards[21]). This will ensure that Europe does not put a limit on the ability of organisations to scale globally. Thus, the data strategy should call for a truly global approach to standardisation (i.e. one that is market-led, takes into account existing standards and with an eye towards interoperability).

- **Data governance**: CIPL supports the Commission's view that for data spaces to become operational, organisational approaches and structures are needed that enable data-driven innovation on the basis of the existing legal framework (see discussion under Section 5).

- **Empowering individuals to exercise their rights**: The strategy notes that while individuals value the high level of protection granted by the GDPR and ePrivacy legislation, they suffer from the absence of technical tools and standards that make the exercise of their rights simple and not overly burdensome. In addition, the strategy outlines that there are calls to give individuals tools and means to decide at a granular level what is done with their data through consent management tools, personal information management apps as well as data cooperatives. CIPL believes that the GDPR provides effective standards and mechanisms for empowering individuals and enables appropriate tools for them to exercise their rights. In fact, CIPL's recent input to the Commission's consultation on the evaluation of the GDPR found that one of the key benefits of the GDPR to date has been driving organisations to deliver more user-centric and contextual transparency to individuals, and to reassess or build effective processes, tools and dashboards for responding to individual rights requests. The Commission could highlight this benefit both in its GDPR evaluation report and within the data strategy and encourage continued and further development of processes for the exercise of rights. A call for the creation of further technical tools in line with GDPR standards is appropriate in this regard.

  With respect to calls for tools and means for individuals to decide what is done with their data at a granular level, CIPL recommends that such tools should only be created where consent is effective and appropriate, and that organisations look to other means for protecting and empowering individuals through organisational accountability in other circumstances. A general call for consent and personal information managers across the board and in all data processing contexts may conflict with the Commission's aim of ensuring technical tools that make the exercise of individual rights simple and not overly burdensome. There are many contexts and circumstances in the modern information age in which obtaining consent can be impractical, impossible, ineffective or not meaningful. For example, (1) where there is no direct interaction with individuals, (2) where the data use is common, trivial and imposes no real privacy risk, (3) where large and repeated volumes of data are processed (seeking consent at every instance may not be feasible or may be meaningless as a result of consent fatigue) or (4) where obtaining consent would be counterproductive such as where data is processed to prevent fraud or crime, or ensure information and system security.[22] Rather than place the burden only on individuals to manage their own data and allow or disallow uses, the strategy should call for accountability from organisations to protect data as they use and share it

through implementing an accountable privacy management program and reliance on accountable data sharing frameworks (see Section 5 below). Furthermore, in instances where consent is appropriate but not obtainable, true anonymisation and/or aggregation might be applied to ensure individuals cannot be re-identified.

Section 5: The Strategy

A. A cross-sectoral governance framework for data access and use

CIPL supports the Commission's approach to deliberately abstain from overly detailed, heavy-handed *ex ante* regulation in crafting a cross sectoral governance framework. The data sharing economy is still developing and will likely evolve and change over time and prescriptive horizontal rules may not be fitting for certain vertical sectors. A governance approach based on demonstrable and enforceable organisational accountability can ensure the necessary protections for data and individuals while enabling innovation through accountable and responsible data sharing. CIPL has written extensively about the concept of organisational accountability in data protection.[23] The essential elements of accountability, integral to effective privacy compliance programs, can facilitate responsible data sharing between and among public and private organisations and should form the foundations of any enabling framework for the governance of common European data spaces.

The essential elements of accountability and their relationship to data sharing include:

- **Leadership and oversight**: For many organisations, data sharing is an important value in the same way compliance is. Creating a successful culture of innovation through responsible data sharing requires leadership from the top in order to realise this ambition while ensuring executive level oversight of and accountability for data processing and sharing activities. In addition to internal leadership, oversight may also include external or internal data review boards and advisory bodies, that would be able to examine and assess a proposed data use and sharing initiative, based on specific criteria (e.g. high risk, large scale, public sector involvement, etc.)

- **Risk assessment**: Responsible data sharing involves identifying potentially risky and impactful data sharing and mitigating the identified risks as a matter of priority before engaging in the data sharing activity. Part of the risk assessment also involves assessment of the benefits of the data sharing project and consideration of reticence risk, or the opportunity cost of not engaging in the data sharing. 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). All of these factors are integral to the risk assessment formula. Conducting such assessments can be done through various means – it could form part of a DPIA for high risk processing or be carried out through a specific data sharing impact assessment where appropriate, through engaging internal or external data review boards or by implementing technical measures such as differential privacy, anonymisation or pseudonymisation techniques.

- **Policies and procedures**: For organisations to share data in an accountable way, they must implement policies and processes such as those concerning (a) requirements for data sharing, data protection, security, intellectual property and other controls and safeguards;

(b) the choice of and due diligence on data sharing partners, vendors and other recipients; (c) requirements of data sharing agreements, especially controller-to-controller, and the ongoing management of third party relationships, including ongoing oversight of agreed data sharing practices and procedures for the escalation and resolution of issues.

- **Transparency**: In many circumstances, individuals whose data is being shared must be given user-friendly information about the data sharing project and how their data will be used, including information about the value of the data sharing project to the individual and/or for society. This is critical to build trust, provide individuals with an opportunity to ask questions and to exercise their data protection rights. In other contexts, where data is being shared for social good and research, it may be appropriate to provide public facing transparency to society as a whole about the project. Transparency also means providing appropriate information to relevant regulators about data sharing projects in response to any queries and investigations, as well as proactive sharing of some information with regulators and other oversight bodies, such as data review boards.

- **Training and verification**: Sharing data responsibly requires training staff about the implications of data sharing and their roles and responsibilities in delivering accountability measures, as well as ensuring they are up to speed on data sharing best practices. The roles and responsibilities of contractors and third parties working on any data project must also be made clear.

- **Monitoring and verification**: Organisations must verify that they are implementing all the requirements, controls and accountability measures set out in data sharing agreements and in line with their own internal governance framework for sharing data. This can be achieved through internal or external audits or through engaging data advisory councils or review boards.

- **Response and enforcement**: Accountable organisations must ensure that they have procedures and controls in place to act upon findings of audits and reviews, address enquiries from regulators and requests and complaints from individuals as it relates to their data sharing activities. Internal enforcement against non-compliance is critical to maintaining an accountable data sharing framework that is robust and adhered to throughout the organisation.

Regarding the Commission's proposal for an **Implementing Act on High Value Data Sets**, CIPL supports the Commission's efforts to make high-quality public sector data available for re-use and appreciates the focus on SMEs as key players in the data economy. A governance approach based on accountability, as described above, can work equally well for ensuring that SMEs share data responsibly. It provides a framework that is risk-based and can be tailored and scaled to the size and nature of the organisation in question, as well as the level of risk they create for individuals and society, which is one of accountability's key benefits.

With respect to the Commission's **Data Act (2021)** proposal to explore the need for legislative action on issues affecting relations between actors in the data agile economy, CIPL recommends:

- **Incentivising organisations to implement accountability** by enabling certain data sharing projects for those that do, taking accountability measures into consideration as a

mitigating factor in cases of enforcement and enabling conditions for public procurement processes which affords opportunities to incentivise best practices.

- **Addressing issues related to usage rights for co-generated data holistically** with reference to the GDPR as well as intellectual property and competition law;

- **Facilitating voluntary data sharing** that is properly incentivised and articulates tangible benefits to all participants. The Commission proposes that the Data Act (2021) could make access to data compulsory where specific circumstances so dictate. CIPL recommends that the Commission first promote and incentivise voluntary sharing arrangements and understand their sufficiency and effectiveness for accountable data sharing before considering compulsory data sharing schemes.

- **Providing for innovative regulatory oversight**, including through regulatory sandboxes and data review boards. In line with the recommendations of the B2G HLEG, CIPL supports the creation of regulatory sandboxes which can provide appropriate avenues to increase data sharing between business and governments. Regulatory sandboxes are not limited to B2G relationships but can be useful for data sharing between all stakeholders where the public interest and complexity of the proposed initiative require additional regulatory feedback and reiterative compliance solutions. Such supervised spaces would provide an additional layer of accountability and supervised experimentation and regulatory feedback as data flows from the private to the public sector. Regulatory sandboxes are currently being employed in the data protection field. The UK ICO is currently concluding the first year of its own pilot phase which may provide useful insights for data sharing sandboxes[24] and the Norwegian DPA has just announced government funding for its own regulatory sandbox in the field of AI.[25] Data review boards may also serve as an agile oversight tool to help organisations 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 sharing initiatives detached from commercial interests. Both regulatory sandboxes and data review boards should be encouraged and incorporated within the Data Act (2021) for the benefits they can bring in enabling the new world of data in responsible ways.

Finally, in creating a cross-sectoral governance framework, the data strategy should call for clarity on the relationship and potential tensions between personal data protection regimes such as the GDPR and other legal data sharing instruments such as the Regulation on the free flow of non-personal data.[26] These tensions may be heightened in the data sharing context due to ongoing debates over what kinds of information constitute personal data, including in the case of anonymised and de-identified data. Furthermore, some data protection obligations are triggered regardless of whether data is personal or not (e.g. ePrivacy rules) and thus the role of anonymisation becomes even more complex in such situations. The strategy should also call for clarification and an update of the existing guidance[27] on how to deal with mixed data sets consisting of both personal and non-personal data in the data sharing context.

B. Investments in data and strengthening Europe's capabilities and infrastructures for hosting, processing and using data

CIPL supports investment in data sharing tools, infrastructures, architectures and governance mechanisms and encourages the EU make such investments to further the development of an accountable data sharing framework. With respect to cloud infrastructures, specifically, it is critical that the data strategy and the proposed cloud rulebook account for the global nature of cloud services. Any type of data residency requirement or obligation to store data in Europe would raise several challenges and hinder the ability of European organisations to innovate.

C. Competences: Empowering individuals, investing in skills and in SMEs

CIPL does not believe that a formal review of GDPR provisions is necessary at this stage[28] and by extension recommends against amending the existing data portability right under the GDPR. CIPL recommends that the strategy instead call for the development of practical ways for individuals to exercise the portability right. Apple, Facebook, Google, Microsoft and Twitter have been working on such an effort through the Data Transfer Project.[29] In addition, the strategy should call for clarity on the parameters of the existing data portability provision and for answers to key questions around what types of data are portable, issues around porting data where multiple individuals are involved, responsibilities of transferors and recipients of ported data, etc.

Investing in skills and general data literacy is of the utmost importance to ensuring the success of the data strategy. Making data available and promoting accountable data sharing is just one part of the puzzle as data in and of itself is not the sole enabler of innovation. Technical skills, awareness and training play a critical role in digital transformation and the strategy should address strategies for upskilling in the areas of AI, machine learning, analytics and cloud computing.

D. Common European data spaces in strategic sectors and domains of public interest

The Commission states that it will promote the development of common European data spaces in strategic economic sectors and domains of public interest and that the horizontal framework will be complemented by sectoral legislation for data access and use, and mechanisms for ensuring interoperability. CIPL believes that in creating common European data spaces, any sectoral frameworks should align with the cross-sectoral horizontal framework based on organisational accountability. As with the proposed Data Act (2021), any new sectoral legislation should not compel organisations in a specific industry to involuntarily share data at this stage. The strategy should call for voluntary EU data spaces and organisations should be able to continue to rely on contracts to give effect to data sharing arrangements.

Section 6: An open, but proactive international approach

CIPL appreciates the Commission's recognition that international data flows are indispensable for the competitiveness of European companies. CIPL supports the creation of a framework to measure cross-border data flows and estimate their economic value within Europe and between Europe and the rest of the world. As previously mentioned, data sharing is a global activity and the Commission must keep this at the forefront in designing Europe's data strategy. While efforts to attract the storage and processing of data in Europe from other countries and regions is a legitimate ambition, it is important that Europe's approach does not lead to an insular data society. Europe's rules on exporting data have

served it well in ensuring that protections travel with data and it is important to recognise that some activities (e.g. running fraud tools globally in real time) cannot be conducted in a segregated manner. Therefore, Europe should incentivise foreign companies to store their data in Europe through differentiating itself in the market rather than through any forms of compelled data sharing or data residency requirements. The EU Commission should continue its policy of engaging in international diplomacy to discourage and disincentivise data localisation requirements of other countries.

Conclusion

CIPL is grateful for the opportunity to respond to the European Commission's consultation on its European Strategy for Data. If you would like to discuss any of the comments in this paper, please contact Bojana Bellamy, bbellamy@huntonAK.com; Nathalie Laneret, nlaneret@huntonAK.com; or Sam Grogan, sgrogan@huntonAK.com.

References

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A European Strategy for Data, 19 February 2020, available at https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[4] CIPL Response to the EU Commission Consultation on the Evaluation of the GDPR, 28 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.

[5] The Irish DPC stated in February 2020 that from Q2 2020 it "will be encouraging applications for Certification schemes and Codes of Conduct". The European Commission should encourage all DPAs to start working on these frameworks without delay in the data strategy. See Irish DPC, Operationalising accountability through Codes of Conduct and Certification, 7 February 2020, available at https://www.dataprotection.ie/en/news-media/blogs/operationalising-accountability-through-codes-conduct-and-certification; Moreover, the EDPB has issued opinions on the accreditation requirements for certification bodies and code of conduct monitoring bodies to several Member States. Member States should continue working on the process to ensure the functioning of both mechanisms. See https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_fr.

[6] See CIPL White Paper on Key Issues Relating to Standard Contractual Clauses for International Transfers and the Way Forward for New Standard Contractual Clauses under the GDPR, 7 August 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_scc_final_paper.pdf.

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046.

[8] The Dutch DPA even considers that absolute anonymisation is impossible. See Dutch DPA press release on use of telecom data in the fight against COVID-19, 1 April 2020, available at https://autoriteitpersoonsgegevens.nl/nl/nieuws/gebruik-telecomdata-tegen-corona-alleen-met-wet.

[9] See FTC 2012 Report "Protecting Consumer Privacy in an Era of Rapid Change – Recommendations for Businesses and Policymakers", available at https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy at page 21.

[10] EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, 21 April 2020, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf.

[11] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32003L0098&from=EN.

[12] European Commission Study on data sharing between companies in Europe, April 2018, available at https://op.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1.

[13] Review of the two Horizontal Block Exemption Regulations, European Commission, available at https://ec.europa.eu/competition/consultations/2019_hbers/index_en.html.

[14] Privacy Preserving Contact Tracing, Apple and Google, available at https://www.apple.com/covid19/contacttracing.

[15] FedEx and Microsoft join forces to transform commerce, 18 May 2020, available at https://news.microsoft.com/2020/05/18/fedex-and-microsoft-join-forces-to-transform-commerce/.

[16] COVID-19 Community Mobility Reports, Google, available at https://www.google.com/covid19/mobility/.

[17] Reiter, J., "Correct use of telco data can help in this crisis", Vodafone Group, 27 March 2020, available at https://www.vodafone.com/covid19/news/correct-use-of-telco-data-can-help-in-this-crisis.

[18] High Resolution Population Density Maps, Facebook Data for Good, available at https://dataforgood.fb.com/docs/covid19/.

[19] Broszio, S., "Corona prediction: Telekom supports RKI", 18 March 2020, available at https://www.telekom.com/en/company/details/corona-prediction-telekom-supports-rki-597114.

[20] Towards a European strategy on business-to-government data sharing for the public interest, European Commission High Level Expert Group on Business to Government Data Sharing, 2020, available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64954

[21] See, for example, ISO/IEC 39794 Series, Information technology — Extensible biometric data interchange format, available at https://www.iso.org/news/ref2478.html.

[22] See "Are Our Privacy Laws Asking Too Much of Consumers and Too Little of Businesses?", CIPL Blog – A Very CIPL Solution: Perspectives on effective and accountable data use, governance, data protection and privacy, 13 December 2019, available at https://www.informationpolicycentre.com/cipl-blog/are-our-privacy-laws-asking-too-much-of-consumers-and-too-little-of-businesses.

[23] See CIPL white papers on The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society, 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf; Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability, 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf; CIPL Accountability Q&A, 3 July 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_q_a__3_july_2019_.pdf; and What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework, May 2020, available at https://www.informationpolicycentre.com/organizational-accountability.html.

[24] The Guide to the Sandbox (beta phase), UK ICO, available at https://ico.org.uk/for-organisations/the-guide-to-the-sandbox-beta-phase/.

[25] A regulatory sandbox for the development of responsible artificial intelligence, Datatilsynet, May 2020, available at https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/en-regulatorisk-sandkasse-for-utvikling-av-ansvarlig-kunstig-intelligens/.

[26] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1807.

[27] Communication from the Commission to the European Parliament and the Council - Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union COM/2019/250 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:250:FIN.

[28] *Supra* note 4 at page 2.

[29] Data Transfer Project, available at https://datatransferproject.dev/.