

Centre for Information Policy Leadership's Response to The EU Commission's Consultation on the Data Act

The Centre for Information Policy Leadership (CIPL)¹ welcomes the opportunity to respond to the Commission's Consultation on the forthcoming Data Act.² As the Commission has consistently recognised, data is a fundamental building block to modern society—essential to providing important services as well as unlocking innovation and value through big data, artificial intelligence (AI) and other emerging technologies. The Data Act is key to improving data sharing and availability as part of the broader European Strategy for Data.

CIPL commends the Commission's continued emphasis on data-driven innovation and agrees with the Commission regarding the importance of promoting business-to-business (B2B) and business-to-government (B2G) data sharing. CIPL also supports the broader effort to clarify legal responsibilities and address historical barriers for B2B and B2G data sharing while upholding privacy and data protection. Creating a data ecosystem that promotes access to data and the use of data for the public good while protecting both privacy and intellectual property will drive economic growth, innovation, and competitiveness. CIPL has previously provided feedback on the European Strategy for Data³ as well as the proposed Data Governance Act.⁴

1. General Comments on the Data Act and the Broader European Strategy for Data

- **Allowing Time for Innovation:** The technology sector is still innovating around data services and collaborative data spaces. Organisations have made substantial strides towards a better understanding of how data can be used by the public and private sector to advance the public good, and efforts that support greater data availability are an important part of this goal. These strides have been made through collaboration between many different actors from businesses, universities, research organizations, and countries around the world. The EU must continue to further promote that collaborative approach to unlock the full potential of data and innovative technologies. The market for data sharing is still in its infancy, and it is important to understand how companies and governments are using and sharing data, generating insights, and leveraging the power of those insights. A study of various use cases and collaborative models can support further innovation and development of best practices.

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 [Data Act & amended rules on the legal protection of databases](#), Public consultation (2021).

³ [CIPL Response to the EU Commission Consultation on a European Strategy for Data](#), 29 May 2020.

⁴ [CIPL Response to the EU Commission's Consultation on the Draft Data Governance Act](#), 5 February 2021.

- **Establishing and Assessing Outcomes:** Data sharing responsibilities of organisations and outcomes sought should be developed with various stakeholders and in accordance with other government and industry efforts. Clear outcomes and expectations should be established and periodically evaluated to ensure that data sharing is serving its intended purpose.
- **Supporting Industry-Led Efforts:** In many of the topics surveyed by the questionnaire, there are regional and international efforts—often led by industry—to develop solutions and best practices to emerging questions. These standards are designed to be flexible and to foster innovation without being too prescriptive, while helping achieve outcomes on transparency, privacy, cybersecurity, safety, and resilience in a global market. CIPL urges the EU Commission to further support those efforts and allow for their continued development and innovation. In some cases, specific legislative action may be premature or may have unintended restrictive consequences.
- **Promoting International Collaboration:** CIPL encourages the EU Commission to approach the Data Act with the consideration that it will be used as global blueprint for lawmakers and regulators already examining issues around data spaces, data availability, and data sharing. CIPL would encourage further exploration of how the EU intends to collaborate on an international level. Globally consistent rules or principles would create efficiencies for the data ecosystem and benefits for various stakeholders, including greater clarity to individuals in understanding what their rights are. Without a carefully coordinated approach, organisations operating internationally may face a complex and potentially conflicting set of rules.⁵ Having fragmented rules across different regions risks adding complexity and creates the possibility for confusion. Having a single set of global principles may help to support consistency, drive confidence, lower costs, and enable competition.
- **Aligning Legal Regimes and Other EU Initiatives:** The Data Act is part of a multi-faceted effort to promote common European data spaces and improve data sharing and availability. It is important to clearly define the distinct purpose of the Data Act in the context of these on-going initiatives to avoid confusion or conflicting obligations. Further, the Data Act should be fully aligned with current law, and in particular the GDPR, the Platform to Business regulation,⁶ and other relevant laws. For individual-level data that is not anonymized, individuals must be able to exercise their right to transparency, access, rectification, objection, and deletion in accordance with the GDPR.
- **Adopting an Agile and Future-Proof Approach:** The Data Act—and the broader effort within the European Strategy for Data—are meant to be the backbone for promoting innovative data spaces within the EU, providing the foundation for facilitating data access and availability needed to promote data-driven innovation. As such, it must avoid being too prescriptive and maintain agility and flexibility to adapt to future innovations and technologies.

⁵ This is important for the Data Act as well as other initiatives in the EU, such as the regulation of AI. See [CIPL Response to the EU Commission's Consultation on the Draft AI Act](#), 29 July 2021.

⁶ [Regulation 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.](#)

- **Embedding a Principle-based Approach:** To provide an agile and flexible ecosystem, CIPL recommends the data-sharing framework be limited to defining principles that organisations must adhere to, have to implement internally and demonstrate compliance externally (accountability principle). This would enable organisations to implement a comprehensive data governance program that would operationalise these principles into concrete, risk-based, demonstrable and verifiable actions tailored to the context of the data sharing activity.⁷

2. Comments on Specific Issues in the Data Act Consultation Questionnaire

I. B2G data sharing for the public interest

- **Facilitating Data Sharing for the Public Interest:** CIPL agrees with the High-Level Expert Group’s Report on B2G Data Sharing,⁸ which highlighted the benefit of a data-sharing ecosystem that facilitates easier access to data of public interest. Public authorities can use such data to provide a multitude of benefits to society, including data-driven policymaking and decision-making as well as new scientific insights and solutions to societal challenges such as climate change, natural disasters, and health emergencies.
- **Providing for Clear Definitions:** There is a need for (1) a clear definition of what “public interest” means and (2) spelling out when data may be collected and how data may be used for the public interest. B2G data sharing can help unlock important public benefits in certain situations, as demonstrated aptly by the response to the COVID-19 pandemic. However, defining “public interest” and “public sector” will be necessary to provide the scope of scenarios where data may be shared and how data may be used in those contexts. It is important to have a legally sound and precise definition of “public interest” that allows for a clear understanding of what is considered to be “evidence-based public service delivery and policy-making.” Public interest may also need to be considered with respect to privacy and security concerns as well as competition issues. Often, companies commercialise data services and licensing services to the public sector, so drawing clear lines for what constitutes the public interest will be necessary to avoid unintended consequences or overreach.
- **Avoiding Mandatory Data Sharing:** Mandatory data sharing can create a variety of privacy risks, uncertain liability, and potential conflicts of laws. It may also make it difficult to uphold certain data protection rights. For example, if an individual user deletes or corrects data stored by a business after the B2G sharing has already occurred, it may be difficult to ensure that the deletion or correction get promulgated through the whole chain. It is currently also unclear what kind of infrastructure may be needed to store, process, and provide transparency about data sharing activities. Compulsory data sharing, if any, should apply only in very specific and limited circumstances, with clear requirements for fairness, transparency, reasonableness, and non-

⁷ CIPL has published extensively on the topic of accountability. Most recently, CIPL advocated for an emphasis on accountability in its Response to the EU Commission Consultation on the Draft Data Governance Act. See [CIPL Response to the EU Commission’s Consultation on the Draft Data Governance Act](#), 5 February 2021, p. 11-13.

⁸ [Towards a European strategy on business-to-government data sharing for the public interest](#), HLEG Report on B2G Data Sharing, 2020.

discrimination, taking into account privacy, security, protection of business secrets and intellectual property considerations.

- **Supporting Voluntary Arrangements:** B2G data sharing should be accomplished through voluntary arrangements. The result of the particularly challenging landscape of the COVID-19 pandemic demonstrated the promise of voluntary collaboration and voluntary data sharing arrangements. Providing clarification of legal responsibilities and usage obligations for companies and organisations that wish to willingly share data would be a welcome and helpful contribution to promote future collaborations and encourage stakeholder participation in data spaces.
- **Providing for Data Sharing Tools:** One of the impediments to data sharing is a lack of tools to facilitate such sharing, including data sharing contracts, organisational measures, frameworks, and technical tools. Promoting such tools and frameworks would be helpful to encourage data sharing. For instance, standardized data sharing agreements and contracts, such as open data agreements, can help facilitate collaboration by reducing transaction costs, minimizing uncertainties, and standardizing the process for entering agreements. These tools can be developed with various stakeholders, including from the technical community, to identify issues and craft solutions. Accountability frameworks such as the CIPL Accountability Wheel can also foster responsible data sharing practices.⁹
- **Providing for Safeguards:** Data sharing arrangements in B2G scenarios should require proper safeguards to protect privacy and security of data. Anonymization and aggregation of data should be the default preference for shared data. Other safeguards may include data security measures, particularly protecting commercially sensitive information; clear rules on proportionality and reasonableness of the sharing; transparent reporting on how public authorities use the data; limitations on further data usage and clearly defined data retention periods; limitations on secondary sharing of data; and requirements to use privacy impact assessments. Guidelines should be developed with a multi-stakeholder approach.
- **Compensating for Data:** CIPL supports voluntary data sharing with a reasonable and fair compensation scheme. The report of the HLEG on B2G Sharing provides a starting point for continuing further dialogue with industry and other stakeholders to conduct an assessment and provide the structure for fair compensation schemes.¹⁰
- **Need for Skills and Knowledge to Use Data:** Public authorities may lack the data processing capacity needed to adequately organize, examine, leverage, and secure the data that they collect. Although there is an increasing need for data-driven innovation, mandatory data sharing will not address and may outpace this need for capacity building for skills. CIPL encourages the EU Commission to consider solutions that can help increase the technical skillset to improve collaboration.

⁹ [CIPL Response to the EU Commission's Consultation on the Draft Data Governance Act](#), 5 February 2021, page 11.

¹⁰ [Towards a European strategy on business-to-government data sharing for the public interest](#), HLEG Report on B2G Data Sharing, 2020.

II. B2B data sharing

- **Need for Safeguards, Legal Alignment, and Multi-Stakeholder Engagement:** The same principles for B2G sharing are important for B2B sharing as well, including establishing safeguards and frameworks to uphold privacy and data protection rights; ensuring security and integrity; remaining consistent with the GDPR and other legal regimes; and supporting industry and other efforts to establish best practices. Promoting fairness in data sharing and the data economy is also a central component of the Data Act. The fairness test contemplated for B2B data sharing arrangements should be drafted with the collaboration of relevant stakeholders. This can include using the lessons learned and best practices that have emerged in other contexts, such as the open-source community.
- **Providing for Voluntary Arrangements:** It is important that B2B data sharing continue to take place on a voluntary basis, with proper contractual agreements in place and adequate recourse actions. This is important to protect intellectual property rights, trade secrets, and commercial sensitivities. Continued support and exploration of voluntary mechanisms—including the development of tools as discussed above—can help further facilitate data sharing. However, a voluntary approach with an emphasis on contractual freedom should remain the underlying basis for B2B data sharing.
- **Protecting Intellectual Property Rights:** Intellectual property rights are enablers of innovation throughout various sectors, but especially within the tech sector. This includes trade secrets and core business strategies. It is important to ensure that such protections are not weakened or eroded with new legislation. Intellectual property rights and protection of trade secrets should be recognised as an acceptable and legitimate reason for declining a request to share data.

III. Improving portability for business users of cloud services

- **Enabling Industry Collaboration:** Many industry-led efforts, including codes of conduct (SWIPO)¹¹ and standardization (ISO 19441),¹² are working to set guidance and best practices to enable portability of data, so legislative action may be premature. By supporting and engaging in these ongoing efforts, EU policymakers can be instrumental in creating market awareness and generating trust in the cloud market. CIPL recommends collaboration with industry and other stakeholders to further explore policy solutions in this area. As technology and innovation continue to improve, the need for such multi-stakeholder engagement and collaboration will also grow.
- **Strengthening the Right to Data Portability:** Strengthening the right to data portability for businesses, when dealing with cloud providers, could benefit various parts of the data ecosystem. This would allow for instance businesses relying on different cloud providers to share data across

¹¹ After two years of working with various stakeholders, SWIPO AISBL published Codes of Conduct for Infrastructure as a Service (IaaS) and Software as a Service (SaaS). [SWIPO AISBL publishes Codes of Conduct](#), 22 July 2020.

¹² ISO 19441 aims to promote standards to facilitate cloud interoperability and portability. [ISO/IEC 19941:2017 Information technology — Cloud computing — Interoperability and portability](#), 2017.

entities of the same corporate group, allowing for data pooling and facilitating innovation. The use of cloud services with the proper configuration would enable a secure processing environment while still facilitating data sharing and portability in this context.

IV. Complementing the portability right under Article 20 GDPR

- The potential to enhance the portability right, giving individuals more transparency and control over who can access and use their data and for which purpose, can help empower individuals. However, expanding portability should not be so overly broad as to create uncertainty, increase transaction costs, require disproportionate efforts (especially where the right does not present added value to individuals) or hinder innovation. Although it is important to develop industry standards that enable data portability in accordance with Article 20 of the GDPR, it is equally important to balance the issues of interoperability in practice.¹³

V. Safeguards for non-personal data in international contexts

- **Taking Into Account Mixed Datasets:** Most often, organisations will be using mixed datasets that contain both personal and non-personal data and that may be inextricably linked. As the EU Commission noted “[m]ixed datasets represent the majority of datasets used in the data economy and are common because of technological developments such as the Internet of Things (i.e. digitally connecting objects), artificial intelligence and technologies enabling big data analytics.”¹⁴ As the GDPR already strictly regulates the transfer of personal data outside of the EU, adding an additional transfer regime applicable to non-personal data would result in too burdensome, if not unworkable requirements for mixed datasets that could discourage the sharing of data.
- **Developing International Standards:** A growing number of laws are imposing restrictions on data transfers and potentially threatening global trade of data. At the same time, there are ongoing conversations at the international level to set standards for government and law enforcement access to data. There is an increasing need for such global standards and agreements to avoid putting the onus on organizations to assess whether a request is legitimate or whether the legislation applicable in a foreign country is acceptable from an EU perspective. Having clear and widely recognised international standards are instrumental in fostering data sharing activities.

CIPL is grateful for the opportunity to provide feedback and respond to the Commission’s Consultation on the future Data Act. We appreciate the Commission’s consideration of various stakeholders’ views on this important proposal. We look forward to further opportunities to partner with the European Commission on the forthcoming Data Act to build an innovative and responsible data ecosystem. If you would like to discuss any of the comments or recommendations in this response, please contact Bojana Bellamy, bbellamy@huntonAK.com; Markus Heyder at mheyder@huntonAK.com; or Nathalie Laneret at nlaneret@huntonAK.com.

¹³ For further detailed analysis of the right to portability under the GDPR, see [CIPL Response to the Article 29 Data Protection Working Party's "Guidelines on the right to data portability"](#) February 15, 2017.

¹⁴ See [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](#), p. 8-10.