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

Summary of CIPL's Key Recommendations

1. Include **organizational accountability** as a building block of the DGA and upcoming initiatives of the European data strategy, supported by a **light-touch, principles-based and agile regulatory approach to data sharing**;

2. Integrate a **risk-based approach to data sharing** to properly balance benefits, risks and reticence risks to data sharing and to apply the relevant mitigations;

3. Enable **trust across the entire data sharing ecosystem**, including data providers, intermediaries and recipients, whether public or private entities;

4. Enable the **co-design** by regulators and industry of a consistent governance **framework for accountable data sharing**;

5. Promote **regulatory sandboxes to enable responsible data sharing and innovation through** experimentation in consultation with regulators;

6. Clarify the **relationship between the DGA and the GDPR** and provide that Data Protection Authorities (DPAs) are the **sole regulators responsible for matters** regarding personal data;

7. Avoid **overreliance on consent** to the detriment of other available legal bases and the statistical and research exemptions under the GDPR;

8. Ensure a simple, agile and **harmonised approach to request access to datasets and sharing processes across EU Member States;**

9. Clarify the **international data transfer toolkit for non-personal data,** giving consideration to the GDPR experience for personal data transfers to third countries;

10. Enable the use of **cloud services** to promote data sharing while still providing a **secure processing environment**;

11. Create a **level playing field** within and beyond the different mechanisms and approaches to data sharing to enable **both new players and incumbents to innovate and compete**; and

12. Recognise and support the already-existing mechanisms in place that enable organisations to share data in an accountable way for **socially beneficial purposes and in the public interest**.

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

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to the Commission's Consultation on the proposed Data Governance Act (DGA).[2] The DGA is an important step within the EU's broader Data Strategy, as it focuses on facilitating data access and availability while enabling and promoting trust in data sharing. As the Commission has consistently recognised, data is a fundamental building block to modern society—essential to providing important services as well as unlocking key innovations through big data, artificial intelligence (AI) and other emerging technologies.[3] Data sharing and data access have assumed greater importance to help facilitate these innovations, as aptly demonstrated by the global response to COVID-19.

CIPL commends the Commission's continued emphasis on data-driven innovation and agrees with the Commission regarding the importance of data sharing and data availability. CIPL also supports the broader effort to promote the re-use of data collected by public entities for the benefit of the common good. The DGA considers a wide range of issues, using a holistic lens to address availability of data, opportunities to use data for social and economic good, availability of data for small and medium enterprises (SMEs), interoperability, data infrastructure, data protection and cybersecurity. CIPL's Response to the Consultation focuses on the data protection aspects of this conversation, while offering general comments regarding the importance of promoting and facilitating the responsible use and sharing of data. CIPL's comments are applicable to the DGA specifically as well as more broadly to the upcoming proposals of the European data strategy on data spaces, high-value data sets or the future Data Act.

[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 80 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] Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act), COM(2020) 767 final, 25 November 2020.

[3] The DGA clearly emphasizes the importance of data as an underlying purpose for the regulation: "Over the last few years, digital technologies have transformed the economy and society, affecting all sectors of activity and daily life. Data is at the centre of this transformation: data-driven innovation will bring enormous benefits for citizens, for example through improved personalised medicine, new mobility, and its contribution to the European Green Deal." DGA, p. 9.

1. Data Sharing and Availability of Public Sector Data

CIPL supports the DGA's goal of encouraging greater availability of data, both through making public datasets more widely available as well as facilitating responsible data sharing practices.[4] As mentioned in the DGA, addressing the barriers to data access is increasingly important within a data-driven economy, and re-using public datasets can provide one solution. Public datasets by nature are rich, diverse, unique and abundant. The ability to access, use and re-use datasets has widespread societal value and economic benefit, and it is vital to fostering innovation and new business opportunities that are key for the EU recovery plan in the post-COVID-19 era.[5] Indeed, as suggested by the DGA,[6] broadening the use of such datasets will also maximise the benefit of data derived from public expenditures.

The public sector in particular plays an important role in the data sharing ecosystem, and has the opportunity to lead by example. As a key data user and provider, the public sector can contribute to setting high standards for responsible and accountable data sharing throughout the data supply and distribution chains. As the public sector instils measures that ensure the responsible handling of data, the private sector is likely to receive and share more data with public authorities, which in turn can raise trust among all stakeholders—individuals, private-sector organisations and regulators.

Chapter II of the DGA governs the re-use of certain categories of protected data held by public sector bodies. Sensitive public sector data has not been widely available to re-use, even for research or innovation purposes, yet these datasets hold tremendous potential for unlocking public benefits.[7] CIPL welcomes the Commission's recognition that proper safeguards can mitigate risks of making public datasets available for re-use.

CIPL also welcomes the DGA's effort to create a level playing field of actors in the data sharing ecosystem. Article 4 of the DGA prohibits exclusive rights or agreements unless necessary to provide a public service or product in the general interest, and Article 5(2) requires public entities to ensure that conditions for re-use of data are proportionate, non-discriminatory and justified—and further regulates that conditions shall not be used to restrict competition. CIPL commends the inclusion of these provisions as they relate to data held by public sector bodies. This ensures equal opportunity among organisations, promotes competition and welcomes new actors into the data ecosystem.

---

[4] CIPL supports the promotion of responsible practices for data sharing and the overall goal of promoting data governance, but the term "Governance" used in the title of the regulation may create confusion among stakeholders. The primary function of the currently-termed DGA is to foster data availability, and as such—perhaps the "Data Availability Act" would be a more accurate name.

[5] As NextGenerationEU promises: "Post-COVID-19 Europe will be greener, more digital, more resilient and better fit for the current and forthcoming challenges." Recovery Plan for Europe, EU Commission.

[6] "The idea that data that has been generated at the expense of public budgets should benefit society has been part of Union policy for a long time. Directive (EU) 2019/1024 as well as sector-specific legislation ensure that the public sector makes more of the data it produces easily available for use and re-use." DGA, Recital 5.

[7] The benefit of providing access to public sector data has been recognised by other jurisdictions as well. For example, the United Kingdom's Centre for Data Ethics and Innovation acknowledged the benefit of public sector data to scientific research and the public benefit in its independent report "Addressing trust in public sector data use," CDEI, 20 July 2020.

Although it is important to ensure that sharing and processing environments are secure, CIPL would caution against overly restrictive measures. For example, according to Article 5(4)(a) of the DGA, public sector bodies can impose obligations "to access and re-use the data within a secure processing environment provided and controlled by the public sector." This negates, by default, the possibility of using highly secure environments that are provided by the private sector, such as cloud environments. CIPL encourages the Commission to focus on control of the data rather than the ownership or provision of the underlying infrastructure. We believe that the security protections of cloud environments can be more robust, scalable and cost effective than those available on-premises. This is confirmed by independent research, including the "Cloud Computing Risk Assessment" conducted by the European Union Agency for Cybersecurity (ENISA).[8] Eliminating "provided" from this provision or redrafting this provision to say "provided or controlled by the public sector" would enable the use of cloud services, which would promote data sharing while still providing a "secure processing environment."

Article 5(5) of the DGA entitles public sector bodies to "verify any results of processing of data undertaken by the re-user and reserve the right to prohibit the use of results that contain information jeopardising the rights and interests of third parties." CIPL cautions against this provision, as the possibility for intervention is overly broad. This could create unreasonable barriers or reticence among organisations looking to use public sector data. CIPL recommends using a risk-based approach to determine the appropriate technical and nontechnical safeguards to promote accountability, as discussed further below.

CIPL welcomes the inclusion of Article 5(7), which preserves the right of the database creator by providing: "Re-use of data shall only be allowed in compliance with intellectual property rights. The right of the maker of a database as provided for in Article 7(1) of Directive 96/9/EC shall not be exercised by public sector bodies in order to prevent the re-use of data or to restrict re-use beyond the limits set by this Regulation." The database right protects the investment of the database creator,[9] and as such is geared primarily towards the private sector. Public sector bodies generally do not need to have their investment protected in the same way,[10] as their databases are usually part of fostering a public mission (as opposed to part of an investment or business plan).

[8] Cloud Computing Risk Assessment, European Union Agency for Cybersecurity (ENISA), 20 November 2009.
[9] The Directive provides that "Member States shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database." Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.
[10] CIPL underlines this may not be always the case as there may be a wide variety of situations covered under the term "public sector entity" in different Member States. In addition, some public datasets may not be publicly funded and need to rely on income generated through their use to make them sustainable.

2. Importance of Harmonisation across EU Member States

The DGA is an important piece of the data strategy framework designed to help facilitate data sharing in numerous contexts and relationships. CIPL underlines, however, that data is already regulated through different angles by other existing EU regulations (in particular the GDPR) and would welcome further explanation of how the different regulations are related. The DGA should not overlap with existing regulations so as to avoid confusion among organisations already subject to these regulations, as overlap in the end may result in reticence to receive or share data.

Article 8 of the DGA creates a requirement for EU Member States to establish a single information point for organisations requesting access to public sector data. As the Commission continues to establish procedures for requesting access, CIPL encourages that the process for requesting data under the DGA be simple, efficient and agile for organisations. If the process to gain access is time-consuming or requires long investigative and bureaucratic work for companies, the proposed model of the DGA would risk becoming a bottleneck. Many business models and development schedules that require such data will have a short timeframe, and delays risk stifling innovation. It could also create administrative burdens that affect SMEs and start-ups disproportionately.[11]

To guard against this, CIPL encourages the creation and harmonisation of streamlined processes to work with organisations. Currently, Article 5 of the DGA leaves each public sector body with the responsibility to decide the conditions under which datasets will be available for re-use. This risks potential fragmentation and burdensome complexities for data re-users. CIPL encourages the EU to establish these requirements at the EU level to create a harmonised approach and a consistent set of practices in all 27 EU Member States. This is particularly important for limiting the administrative burden and impact on SMEs. These requirements should detail how datasets will be available, granted or refused by competent national authorities. Absent such harmonisation, there is a potential risk of legal uncertainty and reticence to re-use data.

3. The Need to Resolve Key Challenges of the GDPR and Data Sharing

In addition to the need for streamlined practices across the EU Member States, it is also imperative to provide clarity on the relationship of the DGA with the GDPR. The DGA has multiple points of relation or overlap with the GDPR (for example, personal data under the DGA should only be transmitted for re-use to a third party where a legal basis exists under the GDPR). As mentioned in CIPL's Response to the EU Data Strategy Consultation,[12] as well as CIPL's Response to the EU Commission Consultation on the

[11] *See* Draft Opinion of the Committee on Legal Affairs for the Committee on Industry, Research and Energy on a European strategy for data (2020/2217(INI)), European Parliament (29 October 2020), encouraging that the "new strategy should be implemented by means of a principle-based and innovation-friendly EU legal framework, which should be proportionate and avoid unnecessary administrative burdens for small to medium-sized enterprises (SMEs) and start-ups, and should be combined with concrete measures, guidance, private-public codes of conduct and programmes, strong investments, and, if necessary, new sector-specific laws").

[12] Centre for Information Policy Leadership's Response to the EU Commission's Consultation on a European Strategy for Data, CIPL, 29 May 2020, p. 4-7.

Evaluation of the GDPR,[13] CIPL continues to believe that it is important to resolve key GDPR challenges in order to create and facilitate robust and accountable data governance and data sharing frameworks. Resolving such challenges will help promote trust throughout the data supply chain as well as provide more legal certainty for both large and small organisations. Some of the key areas where there is an opportunity to provide for clarification are summarised below:

***3.1 Differentiating Personal and Non-Personal Data*:** Article 2(3) of the DGA defines non-personal data as "data other than personal data" under the GDPR. This definition may not be always relevant as most often organisations will be using "mixed datasets" that contain both personal and non-personal data and that may be inextricably linked.[14] In some instances, industrial data that may be seen primarily as non-personal data may also be deemed personal data under the GDPR if it relates directly or indirectly to an individual.[15]

The DGA aslo recognises the importance of anonymisation and pseudonymisation as technical approaches that can mitigate associated risks and facilitate information sharing. CIPL encourages the increased use of these techniques and the recognition that anonymisation techniques are contextual and evolving. CIPL welcomes further harmonisation on the interpretation and use of anonymisation across EU Member States.[16] In particular, it is important to recognise that many anonymisation techniques can be coupled with contractual, legal and procedural safeguards to prevent re-identification.[17] Although anonymised data is considered non-personal data under the GDPR, pseudonymised data—as currently interpreted—qualifies as personal data. However, pseudonymised data cannot be attributed to a specific individual and generally pose little risk. In line with the risk-based approach under the GDPR, organisations should be

[13] CIPL Response to the EU Commission Consultation on the Evaluation of the GDPR, 28 April 2020.
[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, COM(2019) 250 final "Mixed 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," p. 8 - 10.
[15] See for example a quality control report on a production line making it possible to relate the data to specific factory workers (e.g. those who set the production parameters), or analysis of operational log data of manufacturing equipment in the manufacturing industry, see 14 at p. 7-8.
[16] EU Member states have not consistently interpreted anonymisation techniques under the GDPR. For example, the Dutch DPA has previously suggested that absolute anonymisation is impossible for certain types of data due to the risk of re-identification. See Dutch DPA press release on use of telecom data in the fight against COVID-19, 1 April 2020. The European Data Protection Board (EDPB) defines anonymisation as "the use of a set of techniques in order to remove the ability to link the data with an identified or identifiable natural person against any 'reasonable' effort. This 'reasonability test' must take into account both objective aspects (time, technical means) and contextual elements that may vary case by case (rarity of a phenomenon including population density, nature and volume of data). If the data fails to pass this test, then it has not been anonymised and therefore remains in the scope of the GDPR." See Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, EDPB (21 April 2020), Recital 15.
[17] See Protecting Consumer Privacy in an Era of Rapid Change—Recommendations for Businesses and Policymakers, United States Federal Trade Commission (FTC), 26 March 2012. The FCT test recognises that in order to achieve anonymisation, organisations often need to combine technical, procedural and legal safeguards.

able to process pseudonymised data with more streamlined procedures, without the full-fledged requirements of the GDPR.

Finally, the GDPR defines personal data as data that relates to a natural person. Personal data can also be "multi-sided" when it relates to more than one individual (for example, a transaction between two parties in the context of mobility pick-up/drop-off location and router details inherently relates to both a driver and a passenger). Coherent approaches to anonymisation and pseudonymisation are even more important in this specific context.

***3.2 Clarification of DGA concepts in alignment with GDPR**:* The concepts of "data holders," "providers," "intermediaries" and "pre-processed data" introduced within the DGA may also cause confusion between existing GDPR concepts of "controller," "processor" or "processing." More clarity would be welcome regarding how these roles relate or overlap, and the GDPR should be the benchmark for defining these roles. It would also be helpful to have clarification on the obligation concerning data processing agreements for data intermediaries in relation to Article 28 of the GDPR. As mentioned above, it is important to promote harmonisation and clarity between the DGA and GDPR to ensure consistency and promote legal certainty.

3.3 Progressive Interpretation of Key Data Protection Concepts: The GDPR is principles-based and designed to be adaptable to new uses of data and data sharing. Promoting a data-driven economy will require progressive and consistent interpretations of key data protection concepts by the EDPB, DPAs, and the new European Data Innovation Board (EDIB). This can be an opportunity to clarify and ensure that key provisions of the GDPR are not interpreted too restrictively. For example, while the DGA requires a legal basis for processing personal data,[18] this should not be interpreted systematically to mean consent. The six legal bases for processing data under the GDPR exist without preference or privilege for one over the other. Although currently DPAs, lawmakers and policymakers appear to place a stronger emphasis on consent, presumably based on a belief that it is more protective and individually empowering, there is a growing need to support broader, flexible applications of other legal grounds for processing, such as public interest as well as legitimate interest, which in fact can provide greater protections to the individual.[19] It is also critical that DPAs provide clarity and ensure that data is available for statistical and research purposes under Article 89 of the GDPR.[20] Overall, as part of the continued effort to eliminate barriers for important data sharing practices, the EDPB, the EDIB and DPAs should consider how to address these issues jointly and consistently in a constructive manner.

[18] "In general, insofar as personal data are concerned, the processing of personal data should rely upon one or more of the grounds for processing provided in Article 6 of Regulation (EU) 2016/679." DGA, Recital 6.

[19] The EDPB clarified last year that private entities aiming to combat COVID-19 may rely on the public interest derogation for cross-border transfers of data used for research purposes. See 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. More of such guidance is welcome to allow for the flexibility needed to promote data sharing for the public good.

[20] Clarity around this is needed, as organisations currently report reluctance and caution when using the scientific research exemption, fearing noncompliance based on uncertainty of regulators' expectations. CIPL's Response to EU Data Strategy Consultation, p. 7.

3.4 International Data Transfer Toolkit for Personal Data*:* European data spaces should be developed with an eye on global interoperability and collaboration. Data sharing across jurisdictions will be important to unlocking the benefits of innovation and research, but it must be done while upholding European values. CIPL cautions against any unjustified restrictions to international data flows, which can significantly limit the technology choice of EU data re-users and their potential to innovate. Taking additional steps to contribute to enabling the free flow of data in Europe and beyond is important to avoiding friction for data flows between different jurisdictions. It is imperative, to this end, that the EDPB and DPAs complete the international data transfer toolkit for personal data provided by the GDPR, including standard contractual clauses, binding corporate rules and timely review of adequacy decisions. It is also essential that the EDPB and the EU Commission provide pragmatic guidance to organisations transferring personal data outside of the EU in the aftermath of the CJEU Schrems II decision[21] to enable data sharing activities across borders.

4. International Data Transfer Toolkit for Non-Personal Data

In an effort to protect confidential or non-personal data covered by intellectual property (IP) rights, Article 5(7) and 5(8) of the DGA provides for specific obligations on the re-user of data, including when such data is transferred to a third country (these obligations will most likely be imposed through contractual arrangements). Article 5(9) of the DGA also empowers the Commission to determine whether the legal, supervisory and enforcement arrangements of a third country "ensure protection of intellectual property and trade secrets in a way that is essentially equivalent to the protection ensured under Union law." As the Commission notes, these "essentially equivalent decisions" should take into account long-standing international agreements such as the Berne Convention or the TRIPs agreements that have brought together a number of like-minded countries on the protection of IP rights. In case a specific third country benefits from an "essentially equivalent decision," it seems that the safeguards from the re-user of data required under Article 5(10) of the DGA are not necessary anymore.

These "essentially equivalent decisions" appear to be analogous to the adequacy determinations for personal data made by the EU Commission under Article 45 of the GDPR. CIPL cautions against being too prescriptive with rules for international non-personal data transfers, as organisations already rely on other measures, such as contracts, to protect their data. Drawing on experience from the GDPR, the availability of adequacy decisions is currently limited to a very small number of countries (for example, because of resource constraints). Therefore, CIPL notes that going forward, there should be clarity on which countries will be prioritized for assessment, what the assessment process will entail, and how long the process for adopting such decisions for the types of data covered will be. In addition, in order to further streamline transfers to third countries and taking inspiration from the GDPR, CIPL would recommend that the DGA propose a similar toolkit of Codes of Conduct, Certifications to serve as international transfer mechanisms.

[21] See CIPL Comments on EDPB Supplementary Measures Recommendations; CIPL Comments on Standard Contractual Clauses for Personal Data Transfers under the GDPR; CIPL White Paper on GDPR Transfers Post-Schrems II

5. Embedding a Risk-Based Approach in the DGA

CIPL believes that the DGA should clearly integrate and rely on a risk-based approach to data sharing to assess the risk and determine which safeguards are necessary and appropriate in a particular situation. The risk-based approach to data protection helps to appropriately calibrate protections and controls after considering and weighing the potential risks and benefits of processing data to individuals and society. For example, assessing risk of data sharing to combat COVID-19 necessitates balancing the right to privacy and data protection with the right to life and health, and the corresponding risk of lost opportunities of not sharing data. Not only can risk assessments help guide decisions of whether or not to engage in data sharing, but they can also suggest proper mitigation measures.

A risk-based approach can take into account both technical and nontechnical safeguards, depending on the level of risk. For example, non-technical safeguards—such organisational accountability, engaging data review boards for new projects and other forms of risk assessment and mitigation—can be combined with technical approaches (as recognised in the DGA—anonymisation, pseudonymisation, differential privacy, generalisation, aggregation, etc.) in high-risk settings. Lower-risk situations may only merit non-technical safeguards. Such an approach could be adopted to account for both personal and non-personal data.

It is important to endorse a risk-based approach to data sharing in order to maintain the flexibility needed in a data-driven economy. Certain data is inherently more sensitive and requires greater protection; for example, health data has a higher potential impact on individuals than weather data and should accordingly have higher standards of protection and receive greater attention. Metadata provides another apt example. Article 11(2) of the DGA limits the processing of metadata by data sharing service providers to the development of the service they provide. Yet, metadata may in practice pose little risk to individuals, businesses or public entities. Limiting its use by default may preclude important and beneficial uses of metadata, such as for fraud detection or cybersecurity threat monitoring. Rather than limiting its use, CIPL encourages using a risk-based approach to provide the appropriate level of protection given the corresponding risk of the processing. Risk assessments in data sharing will practically require organisations to properly balance the risks and harms to individuals, the public benefit expected from the data sharing as well as the opportunity cost of not engaging in the data sharing project (reticence risk).

In order to assess potential risks to individuals, organisations should rely on the GDPR methodology based on evaluating the likelihood and severity of harm to individuals They should be able to reuse their existing toolkits under the GDPR to complete these risk-based assessments for data sharing, such as using data protection impact assessments (DPIAs) or other risk assessments tools they have developed.

6. Data Governance, Regulatory Collaboration and Regulatory Oversight

Data governance under the DGA refers to “a set of rules and means to use data, for example through sharing mechanisms, agreements and technical standards. It implies structures and processes to share

data in a secure manner, including through trusted third parties."[22] Thus, the DGA characterises governance as setting up an ecosystem of data sharing service providers, rules to facilitate the safe sharing of public data, and mechanisms to limit risks. CIPL welcomes this broad approach to creating a governance framework to promote data sharing, access and use, as this is an important step to fostering trust that is vital to encouraging and strengthening numerous data sharing relationships throughout the data sharing life cycle. It should also be underlined that data sharing by private sector entities should remain strictly voluntary, with no requirement to make data available (unless of course as legally required under the data portability provisions of the GDPR).

CIPL encourages further clarification regarding the roles of various regulators and oversight mechanisms under the DGA. Chapter VI of the DGA creates a formal expert group, the EDIB, with the goal of facilitating sharing of best practices, promoting interoperability and ensuring consistency across regulations. CIPL welcomes the creation of the EDIB and underlines the importance of working in collaboration with industry and other relevant stakeholders to recognise the intricacies and nuances of different sectors and perspectives. In this fast-evolving ecosystem where technology plays a prominent role, it is essential to rely on the most current industry practices and to create sound and agile guidelines and tools aligned with the latest technological developments.

CIPL agrees that the EDIB should work closely with the EDPB and DPAs to develop a consistent governance framework for accountable data sharing that is protective of individual personal data. It is imperative that the EDPB and EDIB have consistent approaches to interpreting personal data concepts in order to provide legal certainty to organisations and facilitate trust in the data sharing environment. We also suggest cooperation with other European and international bodies to guarantee a harmonised approach on the development of data spaces.

Overall, there is an increasing need for clarifying the roles and responsibilities of various interacting regulatory bodies in the data ecosystem. In the absence of such clarification, CIPL cautions against a multiplication of regulators that could confuse both organisations and citizens. Above all, the DGA should clarify that DPAs are the sole regulators responsible for all matters regarding personal data. Beyond that, it would be helpful to have clear mandates, direction and hierarchy to help promote consistency in interpretations. For example, the new competent authorities under the DGA would manage a number of supervisory requirements, including monitoring compliance of data sharing services, certifying or labelling trusted data intermediaries, and ensuring compliance of registered data altruism organisations. It is important to clarify the roles and responsibilities of these new organisations and their relation to the EDPB and national DPAs.

Finally, CIPL recommends greater inclusion of innovative regulatory oversight mechanisms within the data governance and data sharing framework. For instance, regulatory sandboxes allow for an agile approach to data governance that favours experimentation, iteration and differentiation—a welcome approach

[22] Regulation on data governance – Questions and Answers, EU Commission, 25 November 2020, available at https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2103.

under the EU Data Strategy.[23] These sandboxes can provide a safe space for testing innovative forms and methods for data use and sharing under the supervision of a DPA and/or other regulators as relevant.[24] Regulatory sandboxes can be useful for data sharing between all stakeholders, especially when the public interest and complex nature of the project would benefit from regulatory input and feedback. This would enable supervision, create additional layers of accountability and promote innovation and experimentation for the creation of best practices.[25] Regulatory sandboxes are currently being utilised in other countries for data sharing purposes, such as in the UK,[26] as well as in other fields involving innovative technologies and data use, such as in Norway for the field of AI.[27]

7. The Role of Organisational Accountability

CIPL believes any framework for data sharing should be based on demonstrable and enforceable accountability standards that would enable organisations to make their activities compliant with principles enshrined in the law. In other words, because data sharing activities have to be assessed and their risk mitigated in a specific context, the law should avoid being too prescriptive. It should limit itself to defining principles that organisations must adhere to and have toimplement internally. To do so, organisations must implement a comprehensive data compliance and governance program covering data collection, use, access and sharing. This program enables to operationalise these principles into concrete, risk-based, demonstrable and verifiable actions tailored to the specific data processing activity, including data sharing. Organisational accountability helps to sustain a light-touch, principles-based and agile approach to data sharing. CIPL believes that the DGA should encourage and promote organisational accountability as an effective and useful mechanism for responsible data sharing practices across organisations.

CIPL has published extensively on the concept and implementation of organisational accountability in data protection settings.[28] Organisational accountability can solve or mitigate many of the existing challenges of data sharing relationships, promote trust in confidently sharing data for research and support data for good and for the overall public benefit. It is also relevant across various data sharing relationships

[23] 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, COM(2020) 66 final, 19 February 2020, p. 12.
[24] CIPL examines the potential of regulatory sandboxes in the context of AI and emerging technologies in CIPL's Response to the EU Commission White Paper "On Artificial Intelligence – A European approach to excellence and trust," CIPL, p. 21-22.
[25] CIPL has previously published a white paper on regulatory sandboxes outlining their benefits for organisations, DPAs, individuals, and society as a whole. Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice, CIPL, 8 March 2019.
[26] The Guide to the Sandbox (beta phase), UK ICO.
[27] A regulatory sandbox for the development of responsible artificial intelligence, Datatilsynet, May 2020.
[28] To provide a few examples of the work CIPL has done to promote organisational accountability, see The Case for Accountability: How It Enables Effective Data Protection and Trust in the Digital Society; Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability; CIPL Accountability Q&A; What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework.

considered under both the DGA and the upcoming Data Act, including B2B, B2G, G2B and G2G as well as in specific data spaces.

As organisations seek to implement principles set forth by regulators, they may turn to industry standards and best practices, such as the CIPL Accountability Wheel. The essential elements of accountability are integral to responsible data sharing. These elements, shown in the CIPL Accountability Wheel below, include: 1) leadership and oversight; 2) risk assessment; 3) policies and procedures; 4) transparency; 5) training and verification; 6) monitoring and verification; and 7) response and enforcement.

CIPL Accountability Wheel: Elements of Organisational Accountability

In relation to data sharing specifically, the essential elements of accountability include:[29]

- ***Leadership and Oversight*:** Data sharing requires recognition and buy-in from the leadership level of an organisation. This includes executive-level oversight and accountability for data collection, processing, use and sharing. Oversight may also include external or internal data review boards, advisory bodies or other mechanisms that examine proposed data uses or data sharing initiatives based on established criteria. It also includes creating a culture that promotes responsible and accountable data-driven innovation.

- ***Risk Assessment***: Implementing a risk-based approach to data collection, use and sharing can be done though data protection impact assessments (DPIAs) and through engaging with advisory

[29] These elements were explored further in CIPL's Response to the EU Data Strategy Consultation, p. 13-14.

boards. Risk assessment should include consideration of individual and collective impact, when appropriate, as well as an evaluation of the benefits of data sharing and the reticence risk.

- ***Policies and Procedures***: Having proper policies and procedures in place is a necessary predecessor to being able to share data in a responsible and accountable way. This should include employees' obligations, processes to follow concerning requirements for data sharing and safeguards, due diligence on data sharing providers, partners and vendors, and clearly outlined requirements for data sharing agreements.

- ***Transparency*:** Meaningful transparency is a critical component of building trust, and it may require that individuals be given user-friendly information about data sharing and how data will be used—including, where appropriate, information about the expected individual and societal benefits. In cases of projects in the name of public benefit and research, transparency may also consist in public-facing information about the project.

- ***Training and awareness***: Employees, contractors and third parties should have clearly defined roles and responsibilities with respect to data sharing practices and be properly trained within those roles. Roles and responsibilities should be outlined within the organisational policies and updated to reflect current data sharing best practices.

- ***Monitoring and Verification***: Organisations should conduct audits (internal and external) to verify that their employees are adhering to their policies and contractors comply with their contractual commitments. This also enables to identify potential compliance gaps and to rectify them.

- ***Response and Enforcement***: Organisations should have processes in place for enforcing internally their policies regarding data sharing. They should also have processes to respond to external requests and inquiries from regulators and individuals regarding data sharing practices and as the case may be provide for redress.

As a matter of fact, CIPL welcomes that the DGA includes provisions that have a flavour of organisational accountability as described above. This includes, for example, the obligations for data intermediaries to have procedures in place to prevent fraudulent or abusive practices, to implement adequate technical, legal and organisational measures to prevent unlawful transfer or access to non-personal data and to take measures to ensure a high level of security for non-personal data. Similarly, data altruism organisations are required to provide transparency in their activities. These provisions will help promote responsible practices and trust in the ecosystem given the important role that these intermediaries will play in the data sharing ecosystem.

8. Data Intermediaries

CIPL notes the creation of data intermediaries and data altruism organisations as mechanisms to further enable data sharing. Data intermediaries are envisioned as key actors in the data distribution chain and are poised to set the example and adhere to high standards of organisational accountability, ensuring that procedures, policies and practices align with the promotion of responsible data sharing. Not only are data intermediaries important for facilitating data sharing and data access, but neutral data intermediaries can facilitate data exchanges, incentivise voluntary information sharing and play an important role in upholding data protection rights. For example, data intermediaries can help data users comply with the data subject request provisions of the GDPR.

While acknowledging the important role of data intermediaries and other data sharing service providers, CIPL would welcome more legal clarity on the definition and scope of legal intermediaries. Recital 22 suggests that a data holder, such as cloud providers or advertisement data brokers, cannot be intermediaries and should not be captured under the DGA's rules. CIPL would welcome clarity on this in the operative Articles (namely, Article 9). It remains unclear, however, from the Articles and the Recitals, whether legal affiliates to data holders may act as a data intermediary.

It is also important that the DGA remains coherent with the GDPR provisions when intermediaries process personal data. The large definition of the concept of "processing" under the GDPR[30] captures the intermediaries' activities whenever they are dealing with personal data. It is important that the DGA does not create exemptions or special conditions to the GDPR and that intermediaries operate in accordance with the GDPR when handling personal data. It should also be made clear that DPAs have full and exclusive competence under the GDPR (including its one-stop-shop mechanism) to oversee compliance of intermediaries' activities.

The DGA also creates an obligation that "the provider offering services to data subjects shall act in the data subjects' best interest when facilitating the exercise of their rights, in particular by advising data subjects on potential data uses and standard terms and conditions attached to such uses." It is unclear, however, who defines the data subjects' best interests and how that determination would be made. It is key that in any case this be performed in full alignment with the GDPR and EDPB guidance.

Overall, data intermediaries will need to operate in a framework that is scalable and creates value. Rather than mandating the use of a data intermediary, which could discourage sharing and stifle innovation, the data sharing ecosystem should create a level playing field within and beyond the different mechanisms and approaches to data sharing to ensure that no existing or new participant is unintentionally preferred or barred. Such a framework would enable both new players and incumbents to innovate and compete. While data intermediaries can further enable data sharing, CIPL underscores the need to recognise and support these in addition to already-existing mechanisms that organisations are using to responsibly share data.

[30] Article 4(2) of the GDPR defines processing as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

9. Data Altruism

CIPL appreciates the DGA's goal of facilitating a concept and framework for data altruism—"the consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services."[31]

However, it is vital to define data altruism in such a way that does not collide with or undermine the existing legal bases and exemptions under the GDPR. For example, the GDPR already includes public interest and research purposes as legal bases for processing. Clarifying these concepts is especially important given the confusion that already exists when interpreting the GDPR's legal bases—in particular, when considering the unjustifiably privileged role that is given to consent over other legal bases where, under the terms of the GDPR, all legal bases are supposed to be on an equal footing. Rather than relying on consent exclusively, it is important to promote such data sharing within a trustworthy and accountable framework that places the onus on organisations to effectively protect individuals by appropriately identifying, addressing and mitigating risks.

As mentioned above, it is also important to recognise that many organisations are already sharing data for the public interest, adhering to strict ethical, security and privacy concerns. Data altruism and data intermediaries have the potential to be important additions to the data sharing ecosystem, but there are other mechanisms in place that enable collaboration in an accountable way for socially beneficial purposes. CIPL recognises the potential of data altruism organisations as one piece of this broader ecosystem while also encouraging further recognition and development of data sharing best practices for data uses for the public benefit.

Conclusion

CIPL appreciates the Commission's consideration of various stakeholders' views on this important proposal and is grateful for the opportunity to provide feedback on the DGA. This is an important step within the broader European data strategy on data spaces, as it will enable data sharing and promote best practices that can serve as a basis for future legislation. We look forward to further opportunities for dialogue on responsible and accountable data sharing.

If you would like to discuss any of the comments or recommendations in this response, please contact Bojana Bellamy, bbellamy@huntonAK.com; Nathalie Laneret, nlaneret@huntonAK.com; or Markus Heyder at mheyder@huntonAK.com.

[31] DGA, Article 2(10).