Computer & Communications Industry Association
Tech Advocacy Since 1972

Data Governance Act
CCIA Europe comments

Executive summary

The Computer & Communications Industry Association ('CCIA Europe') welcomes the objectives of the proposed Data Governance Act ('DGA'), as a vehicle for greater data sharing between companies, public sector bodies, and individuals.

CCIA Europe remains a staunch supporter of policies fostering greater public and private data sharing that may contribute to social improvements and economic innovations in Europe. We agree that trust and legal certainty are essential for encouraging greater data-sharing among public and private organisations and citizens, especially when the data involves trade secrets, IP protected information, and personal data.

But it is also important to ensure that the EU's data-sharing rules remain open and non-discriminatory towards all market participants, proportionate to the public policy objectives sought, and consistent with existing EU domestic laws and foreign policies. Last but not least, meaningful incentives should be considered to fulfill the primary objective of this proposal, i.e. fostering data sharing in Europe.

Overall, CCIA Europe is concerned that the proposed regulatory framework would inhibit data sharing in Europe. We observe a number of undue restrictions which at best appear counterintuitive if the goal is to promote data sharing and further use. At worst, it could legitimise similar restrictions that European companies face abroad. In addition, we invite lawmakers to consider improving the proposal through meaningful incentives for market participants to share, access, and use each other's data, and to provide data intermediation services.

CCIA Europe invites lawmakers to improve the proposal, and focus on:

- **Fostering meaningful safeguards conducive to a trusted environment for data-sharing in Europe while avoiding isolationist, counterproductive measures.** On the other hand, lawmakers should refrain from adopting data transfer restrictions and otherwise similar measures that would be ineffective, stifle data sharing in Europe, undermine EU's acquis and trade agenda;
- **Clarifying the scope of "providers of data sharing services" and introducing incentives** to ensure effective market competition among those providers, for the benefits of data holders and users;
- **Ensuring that third party access does not undermine data holders' interests and rights** (statutory, licensing or otherwise);
- **Incentivising public sector digital transformation.** The DGA should ensure that the prohibition of exclusive agreements does not contravene with normal B2G practices, and should refrain from enshrining any form of in-house, localised processing by public sector bodies.

1. Meaningful safeguards to foster data-sharing and avoid isolationist measures

CCIA Europe supports the complementary objectives of (1) fostering a trustworthy environment that is conducive to (2) greater data sharing in Europe. That is why we are concerned to see that some of the proposed measures, such as data transfer restrictions, would be ineffective to reinforce trust and stifle data sharing altogether. Similarly, we caution against establishing a unilateral adequacy framework which, after 25 years of track-record in the field of data protection, has proven slow and burdensome to manage, unfit to ensure global data flows for European and international organisations, and risks creating double-standard vis-a-vis EU's trade partners.

CCIA Europe invites EU lawmakers to remove any form of undue data transfer restrictions in Article 5(4), Article 5(11) and corresponding recitals. Similarly, we cautions against a burdensome adequacy-like framework for non-personal data in Article 5(9). Instead, we invite EU lawmakers to consider the robust set of EU legislation that service providers, public bodies, and data re-user must already comply with to ensure that sensitive public, commercial, and personal information are adequately protected and to prevent undue access, use and disclosure of personal and non-personal data. To facilitate compliance with Article 30, the European Commission should be empowered to issue non-binding guidance on specific situations and examples of (i) laws and practices that would warrant increased technical and organisational measures to safeguard the integrity of non-personal data, and (ii) specific exemption scenarios under Article 30(3).

A) The proposed data transfer restrictions are unjustified, ineffective, incoherent with GDPR, leave customers and vendors worse-off, and jeopardise EU's trade position

Article 5(11) alongside Recitals 19 and 43 contemplate the possibility of a localisation requirement as well as other data transfer restrictions for "highly sensitive data." The proposal does not define what would constitute "highly sensitive data" and leaves *carte blanche* for the European Commission to determine in a delegated act what type of data may be subject to a data localisation requirement or other transfer and use restrictions. In addition, neither the proposal nor its accompanying impact assessment demonstrate why said restrictions may be needed even if they conflict with the General Data Protection Regulation, ignore other applicable legislation (e.g. NIS and Trade Secrets Directive), and undermine the EU's trade agenda. Similarly, we are concerned that Article 5(4) legitimise public sector bodies' data localisation requirements and extend that requirement to third party access and re-use. When combined, these provisions may severely limit public bodies' ability to procure external IT services in practice.

The proposed transfer restrictions lack justification, proper identification of the policy objective(s) pursued

CCIA Europe notes that the proposal does not provide any meaningful justification for such restrictions. Instead it simply and broadly refers to "build[ing] trust", the protection of "legitimate public policy objectives" and the protection of "the public interest."[1] Similarly, the impact assessment only loosely identifies the need for "trust in data-sharing" and dedicates one sentence to "demands to access data by governmental authorities, including from third countries that do not comply with due process requirements."[2]

[1] See Recital 19
[2] Commission Staff Working Document, Impact Assessment Report, SWD(2020) 296 final, p. 20

CCIA Europe wishes to remind that a clear *identification* of the public policy objective(s) sought is the one of the first conditions of lawfulness for any measures that seek to derogate from the General Agreement on Trade and Services (GATS) as per Article XIV and jurisprudence thereof.[3] Vague references such as those found in the proposed DGA and the lack of substantive demonstration that "health data" is inherently highly sensitive and will therefore be subject to data transfer restrictions - including localisation - regardless of any other relevant circumstances, arguably lack a sufficient degree of specificity to qualify as a valid exception under GATS.

Ineffective tools to address legitimate concerns

Notwithstanding the lack of clarity of the public policy objective(s) that the proposed data transfer restrictions pursue, CCIA Europe is cognizant of the concerns that government data access laws raise among customers and policymakers. We note that this is an issue that is also briefly mentioned in the impact assessment accompanying the DGA proposal and the European Commission Data strategy.

However, we wish to draw EU lawmakers' attention to the ineffectiveness of data transfer restrictions to mitigate these concerns as the location of data is becoming increasingly irrelevant for governments to assert their jurisdiction and seek data access in domestic law enforcement and national security matters. Indeed, countries around the world, including in the EU, are increasingly adopting extraterritorial laws whose very purpose is to allow government and law enforcement agencies to seek access to data processed and stored outside their jurisdiction. This is for example the case with the 2nd Protocol to the Budapest Convention, the proposed EU e-Evidence Regulation, or the U.S. CLOUD Act.

From an international perspective, the increasing ineffectiveness of data localisation and otherwise similar restrictions raises serious questions about the *necessity* of such measures under GATS Article XIV and jurisprudence thereof.[4] Similarly, erecting data localisation measures for this purpose would raise equally serious questions of coherence at a time when the EU is finalising its own extraterritorial law enforcement data access legislation (i.e. the proposed e-Evidence Regulation).

Conflicts with the General Data Protection Regulation

Since the DGA would apply to personal data,[5] CCIA Europe is concerned that the proposal would set out data transfer rules that depart from and conflict with the General Data Protection Regulation ("GDPR"). Such conflict would bring considerable uncertainty for entities covered by the both regulations, namely public organisations, their private vendors, data holders, and data users.

---

[3] A compendium of the Article XIV jurisprudence can be found on https://www.wto.org/english/res_e/publications_e/ai17_e/gats_art14_jur.pdf

[4] *Ibid.* 3

[5] Under recital 19 DGA, references to the objective to protect individuals' "privacy and personal data protection", health data held by "actors in the public health system", and mitigating the risks of "re-identification of individuals" infer that personal data may also be subject to data localisation requirements or other transfer and use restrictions.

First, we recall that the GDPR sets out a number of mechanisms to allow for personal data flows in and out of the European Economic Area while ensuring appropriate protections are in place. Among other transfer mechanisms, the GDPR instructs service providers to adopt a range of safeguards that a service provider must implement and calibrate according to all the relevant circumstances surrounding the data transfer.

While the DGA seems to suggest the degree of sensitivity of the data should be the primary consideration for the transfer of personal data outside the EEA, the GDPR and the recent CJEU case-law provide broader range of factors to be considered on a case-by-case basis, including an assessment of the laws of the country of destination and vendors' mitigation measures[6] to prevent unauthorised third party access such foreign government or court requests that would conflict with the level of protection afforded under the GDPR.

CCIA Europe calls on lawmakers to ensure legal coherence and certainty for entities transferring personal data outside the EEA.

Significant trade-offs for European customers and vendors

All the evidence shows that data localisation or otherwise similar measures "impose considerable costs on those forced to abide by [these requirements]."[7] From a customer and end-user perspective, such measures reduce the range of potential vendors thereby decreasing competition in the marketplace, increase upfront costs that are then passed on to customers and end-users,[8] and increase cybersecurity risks.[9] Overall, "stricter data policies have a negative and significant impact on the performance of downstream firms in sectors reliant on electronic data".[10] From a vendors' perspective, domestic data transfer restrictions "barring [or restricting] access to foreign services only invite reciprocal [measures] from one's trading partners",[11] and undermine local vendors' chances of exports.

CCIA Europe regrets to see that the proposal effectively departs from the core principles underlying the EU's Free Flow of Data Regulation[12] and the European Commission's negotiation mandate against data flows restrictions abroad.[13]

---

6 See 'Schrems II' decision in C-311/18, para. 112,113, 121, 134, 146, and para. 3 of concluding remarks

7 Svantesson, D. (2020-12-22), "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines", OECD Digital Economy Papers, No. 301, OECD Publishing, Paris. http://dx.doi.org/10.1787/7fbaed62-en

8 Kaplan, J. and R. Kayvaun (2015), "Addressing the Impact of Data Location Regulation in Financial Services", Centre for International Governance Innovation and Chatham House (Paper Series), Vol. 14, pp. 1-2;

9 Brehmer, J. (2018), "Data Localization: The Unintended Consequences of Privacy Litigation", American University Law Review, Vol. 67/3, p. 930, Export Council of Australia (2018), From Resource boom to Digital Boom: Capturing Australia's Digital Trade Opportunity at Home and Abroad, 2018, p. 33, 35

10 *Do Data Policy* Restrictions *Impact the Productivity Performance of Firms and Industries?*, Martina F. Ferracane, Erik van der Marel, ECIPE, October 2018 available on https://ecipe.org/publications/do-data-policy-restrictions-impact-the-productivity-performance-of-firms-and-industries/

11 Chander, A. and U. Le (2015), "Data Nationalism", Emory Law Journal, Vol. 64/3, p. 714

12 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

13 EC Horizontal provisions for cross-border data flows and for personal data protection (in EU trade and investment agreements) available on https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf

B. The inadequacy of "adequacy decisions"

While the DGA does not prevent the transfer of data to 'non-adequate' jurisdictions, CCIA Europe cautions against establishing a unilateral adequacy-like mechanism such as described in Article 5(9), (10), (12), and (13) of the proposed DGA, similar to the the framework under the 1995 Data Protection Directive and its successor, the GDPR.

We remind lawmakers that the long-standing adequacy framework in the field of (personal) data protection has proven to be a slow and burdensome mechanism to manage and unfit to ensure global data flows for European and international organisations. Adequacy decisions typically require intensive bilateral discussions and expertise in relevant domestic laws and practices that may change over time. That's why there are only 12 adequacy decisions in place in the field of data protection, and only two of them cover the top 10 EU trade partners.[14]

Furthermore, adequacy decisions essentially compare the level of data protection afforded by third countries' laws and practices to the level of protection that the EU, alone, may afford, regardless of the Member States' laws and practices. As recent case-law shows in the Schrems II and LQDN cases,[15] there is a palpable dissonance in terms of the treatment of data flows outside the EU and within the EU, and may further exacerbate EU trade partners' perception of double-standard.[16]

3. Reinforce meaningful protection of non-personal data building on EU acquis

CCIA Europe invites EU lawmakers to remove any form of undue data transfer restrictions in Article 5(4), Article 5(11) and corresponding recitals. Similarly, CCIA Europe cautions against a burdensome adequacy-like framework for non-personal data in Article 5(9). Having said that, CCIA agrees that ensuring the integrity and confidentiality of data and information systems is essential to ensure a trusted environment for data sharing in Europe.

In lieu of ineffective data transfer restrictions and a cumbersome adequacy-like framework, CCIA Europe invites EU lawmakers to **first consider the robust set of EU legislation that service providers, public bodies, and data re-user must already comply with to ensure that sensitive public, commercial, and personal information are adequately protected** and to prevent undue access, use and disclosure of personal and non-personal data.

For instance, the Trade Secrets Directive provides strict conditions for the lawful acquisition, use and disclosure of commercially sensitive information, while the Network and Information Security Directive compels digital service providers, including cloud service providers, to take appropriate and proportionate technical and organisational

[14] Switzerland and Japan are currently the only two countries of the top 10 EU trade partners which benefit from an adequacy decision. Source: Eurostat press release 22/2021, dated from 5 February 2021 available on https://ec.europa.eu/eurostat/documents/portlet_file_entry/2995521/6-15022021-BP-EN.pdf/e8b971dd-7b51-752b-2253-7fdb1786f4d9 and European Commission adequacy decisions page available on https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[15] See joined cases Privacy International, LQDN, and others in C-623/17, C-511/18, C-512/18, C-520/18, and 'Schrems II' decision in C-311/18

[16] '*How* Europe's *Intelligence Services Aim to Avoid the EU's Highest Court—and What It Means for the United States*', by Theodore Christakis, Kenneth Propp, 8 March 2021, in Lawfare blog available on : https://www.lawfareblog.com/how-europes-intelligence-services-aim-avoid-eus-highest-court-and-what-it-means-united-states

measures to mitigate any action that may compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data. The General Data Protection Regulation features similar obligations and provides increased oversight scrutiny of government access and disclosure requests.

With this in mind, CCIA Europe generally **supports Article 30** and believes that it is for those subject to these rules, including their vendors, to ensure that technical measures and contractual guarantees are in place to ensure that sensitive public, commercial, and personal information are adequately protected and to prevent undue access, use and disclosure of personal and non-personal data. **To facilitate compliance with this provision, the European Commission should be empowered to issue non-binding guidance** on specific situations and examples of (i) laws and practices that would warrant increased technical and organisational measures to safeguard the integrity of non-personal data, and (ii) specific exemption scenarios under Article 30(3).

Legal certainty and incentives for data sharing service providers

CCIA Europe supports the European Commission's aim to incentivise voluntary data sharing including through dedicated intermediary services as proposed in the DGA. To achieve this objective however, we believe service providers must have the certainty to know whether they fall in the scope of the regulation and must comply with the requirements set out in Articles 10 and 11. For services that do in fact fall in the scope of the proposal, we caution against a too burdensome regulatory framework and invite lawmakers to consider introducing incentives competition among those service providers and promote the attractiveness of the EU's data sharing scheme.

First, CCIA Europe calls on lawmakers to **clarify which type of data sharing service providers must comply with the notification and other requirements** under Articles 10 and 11, and which providers fall outside the scope of the proposed regulation.

As currently worded under the proposal, Article 9(1)(a) would in effect include the vast majority of services that allow organisations to exchange data with one another. At the same time, Recital 22 excludes "providers of cloud services," "Data exchange platforms that are exclusively used by one data holder," IoT data exchange platforms, "consolidated tape providers", "account information service providers", and value added services e.g. advertisement or data brokers, data consultancies, providers of data products resulting from value added to the data by the service provider. For the sake of clarity and consistency, Article 9(1)(a) should be clarified and explicitly exclude service providers in line with Recital 22.

Second, we invite lawmakers to **consider introducing incentives for service providers captured under Article 9(1)**. As currently worded, Chapter III of the proposal only involves obligations and restrictions for service providers, and the combination of all relevant provisions (notification, creation of a separate entity, monitoring and compliance, and penalties) is such that it could very well disincentivise service providers from either entering the market or maintaining their service as is. A voluntary notification system and the establishment of a public register could help raise the level of attractiveness of the EU's data sharing scheme under DGA. In addition, lawmakers may choose to consider allowing the

use of data for purposes other than to put them at the disposal of data users providing that the data sharing service provider complies with any applicable data holders' sharing conditions (statutory, licensing or otherwise).

Clarify data sharing conditions for public bodies and data-sharing providers to protect data holders' interests and rights

CCIA Europe supports the goal of the proposal to ensure non-discriminatory access to third party data across the proposal. At the same time, all parties involved, particularly data holders, should be able to trust that their data will not be used for purposes that would either conflict with statutory obligations or that would run against the will or interests of the data holder.

With that in mind, CCIA Europe believes that the proposal should maintain the principle of non-discriminatory access to third party data via authorised data sharing service providers, but also ensure that public bodies, data sharing service providers and data users comply with any conditions under which that data was shared with them (e.g. limitations on usage for specific purposes). In other words, "re-users" of the data should be subject to any limitations that the data holder may have contractually imposed or agreed with when the data was shared with the data-sharing service or the public sector body. The current phrasing of "non-discriminatory" is somewhat ambiguous in this respect and does not ensure sufficient contractual flexibility.

Specifically, CCIA Europe recommends **introducing a new requirement in Article 5 and 11 for public sector bodies and data sharing service providers to ensure that data holders' sharing conditions** (licensing, statutory or otherwise) **are met** when accessed by third parties / data users.

Absent this clarification, it would mean that data holders would have to factor in new costs of doing business with authorised services at best. At worst, it would likely disincentivise data-sharing across industry given (i) the possibility of sensitive commercial information being made available to third parties (whether comprised of the data itself, proprietary data containers or formats, or insights into technology that the data may provide), and (ii) the possibility that others could receive an unfair advantage from significant investment made in generating, collecting and processing data.

Incentivise public sector digital transformation

CCIA Europe is concerned that the proposed Articles 4 and 5 would stifle local governments' digitisation efforts across Europe.

First, Article 4(1) appears to rewrite procurement rules and prohibit common agreements between data licensors and public sector body licensees, which may ultimately limit the public sector body's ability to distribute licensed data and specify downstream distribution terms.For example, to protect technical data containing proprietary information about product design, maintenance data, and data originating from the operation of a system that the public sector body holds,

it is normal commercial practice to have agreements between that public sector body and the commercial entity that restrict re-use of such licensed data. **CCIA Europe suggests clarifying that Article 4(1) does not apply to common B2G contracts in practice**.

Second, Article 5(4) would leave each public sector body across Europe to decide the conditions of data re-use, creating risks of fragmentation across the EU and even within Member States. CCIA Europe believes it is **important to harmonise the conditions for public sector bodies to make data available for re-use, and suggest to do so by way of an implementing act.**

Finally, we are concerned that the current wording of Article 5(4)(a) could prevent EU organisations from using cloud technologies which are normally provided by third-parties to unleash the potential of public datasets. Where public sector bodies choose to adopt additional conditions for the re-use of data under Article 5(4), it is important that the Data Governance Act does not enshrine some form of in-house / localised processing by public sector bodies. Instead, the DGA should incentivise the digital transformation of the public sector and refrain from imposing measures that would limit public bodies' ability to procure external IT vendor services in practice.

We believe that the security protections of public clouds can be more robust, scalable, and cost effective than those available on-premise. This is confirmed by independent research including the "Cloud Computing Risk Assessment" conducted by ENISA. Cloud environments should be able to serve as "secure processing environments''. **CCIA Europe encourages lawmakers to focus on *control* of the data vs. *ownership* of the underlying infrastructure.**

***

For further information, please contact Alexandre Roure, Senior Manager, Public Policy, CCIA Europe: aroure@ccianet.org