Computer & Communications Industry Association
Tech Advocacy Since 1972

CCIA Europe Comments on Data Act Inception Impact Assessment

Executive summary

The Computer & Communications Industry Association ('**CCIA Europe**') appreciates the opportunity to provide comments on the policy options which the European Commission ('**Commission**') is considering ahead of its proposal for a new Data Act.

CCIA Europe remains a staunch supporter of policies fostering greater data access and re-use among public and private sectors which can drive social improvements and economic innovations in Europe. We commend the European Commission's goal to create a Single Market for data, where data flows between countries and sectors, and where data is available for use in full respect of European values and rules.

You will find below a summary of our comments to the various policy options under consideration. You can find our supplementary comments from page 3 onwards.

1) B2G data-sharing

CCIA Europe encourages the European Commission to introduce an EU-wide, off-the-shelf, and voluntary B2G data-sharing framework model, in full compliance with existing laws and regulations. Such a framework model would provide legal certainty and facilitate on-going and future negotiations for data-sharing agreements across the EU.

However, CCIA Europe cautions against any form of mandated B2G data-sharing. Any expropriation of companies' investments and subsequent free-riding by public bodies would achieve the opposite of "fairness in the data economy", and raise serious questions about companies' incentives to invest time, technology and resources in collecting, transforming, and enriching datasets.

2) B2B data-sharing

The Data Act should remain proportionate to that objective without disrupting the foundational principles of an open market economy with free competition which creates private economic incentives to invest and innovate in data collection and processing, the fundamental freedom to conduct a business, and the freedom to contract.

CCIA Europe invites the European Commission to consider that any type of B2B data sharing obligation be limited to instances where competition law enforcement cannot address the issue.

3) Data portability for consumer connected products

CCIA Europe cautions against mandating "real-time" and seamless data portability without first taking into account the obvious technical challenges which it raises, including user authentication, data import and export eligibility, data format, and exchange protocols.

CCIA Europe also urges the European Commission to carefully consider the privacy impact that overly broad portability requirements may present for data that reveal information about both sides of a commercial transaction or digital experience.

CCIA Europe encourages the European Commission to facilitate an industry-led Code of Conduct for B2C services, similar to the B2B SWIPO Codes of Conduct. In addition, data portability would be greatly facilitated if service providers had greater legal certainty. This is currently not the case with the 2017 EDPB guidelines on data portability.

4) Cloud switching

CCIA Europe has long supported the SWIPO Codes of Conduct for cloud infrastructure and software switching. It is too premature to either mandate the Codes of Conduct via model clauses, or introduce new legal requirements on cloud service interoperability. The EU should advertise and support the Codes, i.e. by adding them to the upcoming cloud rulebook.

5) Government data access

Extraterritorial government and data access laws are a global phenomenon which require multi-lateral safeguards. Any unilateral measures such as those contemplated under the IIA risk pre-empting and potentially conflicting with the outcome of on-going intergovernmental initiatives such as the 2nd protocol to the Budapest Convention, or the on-going OECD process on principles for government data access.

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

Supplementary comments

Business-to-Government data sharing

CCIA Europe supports a low intensity policy option, consistent with the findings of the B2G Data-Sharing Expert Group. The new Data Act could for instance provide a voluntary governance model for B2G data-sharing, laying down the rights and obligations on data access, use and disclosure of each party, without affecting procurement rules and practices. In practice, the drafting and adoption of a data sharing framework at local and national level is time-consuming for all relevant actors, and requires detailed knowledge about the parties' rights and obligations. An EU-wide, off-the-shelf, and voluntary framework model could help accelerate the take-up of future local initiatives.

B2G data-sharing should be based on clear and targeted frameworks, based on outcome and purpose, developed in cooperation and with the active participation of both public and private sector actors.

However, CCIA Europe strongly cautions against the introduction of a "right of [the] public sector to access privately-held data for a range of defined public interest purposes" or any form of mandated B2G data-sharing. Any expropriation of companies' investments and subsequent free-riding by public bodies would arguably achieve the opposite of "fairness in the data economy", and raise serious questions about companies' incentives to invest time, technology and resources in collecting, transforming, and enriching datasets.

From a privacy standpoint, we caution against mandating third party access/use to personal data that could undermine the principles of necessity, proportionality and data minimisation, and disempower individuals over their personal data. It could also raise considerable liability and compliance issues in practical scenarios. For instance, how would public bodies communicate a data breach to individuals if they have no relationship with each other? How would public bodies comply with an individual's request to delete or rectify his or her data?

Finally, mandatory B2G data-sharing would impeach normal procurement practices and prejudge the upcoming data governance framework for public procurement.

Business-to-Business data sharing

CCIA Europe agrees with the Commission's supporting evidence that B2B data-sharing should be promoted by "privileg[ing] soft policy measures over restrictive regulations, rais[ing] awareness about the concept of B2B data sharing and its benefits, and provid[ing] guidance and financial support to companies that are interested in sharing and re-using data among them" (Study on data sharing between companies in Europe (2016/0087), everis Benelux, 2018).

However, establishing a "B2B fairness test", mandating data access, and generalising FRAND terms for a wide range of B2B data-sharing situations appear to run counter those recommendations.

While the objective to "promote fairness in the digital economy" is laudable, the policy instruments should remain proportionate to that objective without disrupting the foundational principles of an open market economy with free competition which creates private economic incentives to invest and innovate in data collection and processing, the fundamental freedom to conduct a business, and the freedom to contract.

CCIA Europe therefore invites the European Commission to consider that any type of B2B data sharing obligation be limited to instances where competition law enforcement cannot address the issue. The mere fact that a data holder has "stronger negotiating power" should not trigger a B2B data-sharing obligation either. Situations where parties have stronger or weaker negotiating power are inherent to business reality and an open market economy.

As recent debates over FRAND terms for standard essential patents reveal, there is not much agreement on how to set FRAND rates, even where technologies are already being licensed for consideration, have clear use cases, and foreseeable valuations. Mandating FRAND licensing with relation to data which has not been previously commercialised and which has unquantifiable future value, would have significant unintended consequences on private economic incentives on Europe's data economy.

Furthermore, a generalisation of FRAND terms for B2B data sharing may be counterproductive to the extent that other data-sharing governance provides more generous conditions to data users. For instance, open data schemes typically entail free-of-charge access and with little to no restrictions of use. The very notion of FRAND terms denote a licensing commitment that would imply that data holders would, by default, enjoy an intellectual property right over the data they hold. CCIA Europe would caution against inadvertently creating new rules where all data held by the private sector is universally treated as an intellectual property, and where any innovation and research driven by text and data mining would require a licensing agreement.

Data portability for consumer connected products and services

The Inception Impact Assessment contemplates mandating technical interfaces for providers of smart home appliances, wearables, and home assistants to allow real-time portability of users' personal data.

CCIA Europe generally believes that data access and portability play an important role in how individuals control their data. Over the last few years, more and more service providers have rolled out user-friendly interfaces in login environments (e.g. dashboards) in addition to traditional ways of enabling data access e.g. a copy sent by e-mail or available for download. Beyond mere data access, we believe portability empowers individuals to try new services and help them choose those that best suit their needs. As such, portability can facilitate competition among services and contribute to greater market innovation.

However, we caution against mandating "real-time" and seamless data portability without first taking into account the obvious technical challenges which it raises. Broadly speaking, automated porting 'without hindrance' from service to service raises technical issues related to user authentication, data import and export eligibility, data format, and exchange protocols.[1] All this has an impact on the system architectures of

[1] The Data Transfer Project White Paper provides a detailed overview of the technical considerations at play, available on https://datatransferproject.dev/dtp-overview.pdf

the sending and receiving ends. As such, there is no one-size-fits-all solution to portability. In fact, market-led initiatives such as the Data Transfer Project show that data portability tools can only be successful if they are developed incrementally, and with user-friendliness always in mind.

To that end, the Commission may wish to consider facilitating an industry-led Code of Conduct for B2C services, similar to the B2B SWIPO Codes of Conduct.

In addition, the 2017 guidelines of the European Data Protection Board on data portability have cast legal uncertainties and added requirements[2] that are either cumbersome or unrealistic for service providers to effectively implement seamless portability.[3] The revision of those guidelines is necessary if the EU seeks to further promote data portability.

Data portability and service interoperability for cloud services

CCIA Europe has long supported the SWIPO Codes of Conduct for cloud infrastructure and software switching. These Codes of Conduct are the results of an inclusive consensus-building process involving cloud users, including SMEs, and cloud providers. We think the impact of the codes can be improved with better communication and advocacy towards the market by all players involved, including the European Commission. The upcoming EU cloud rulebooks seems particularly apt to achieve that objective.

However, CCIA Europe believes it is premature to either mandate the Codes of Conduct via model clauses, or introduce new legal requirements on cloud service interoperability. The Codes of Conduct are only a few months old, and we invite the European Commission to wait until its review of the Codes November 2022 to assess whether the Codes have had any impact on the market. Furthermore, the Codes of Conduct are meant to be living documents, and codifying the Codes into mandatory model clauses would need to be regularly updated to reflect any future changes as technology progresses.

Data transfers and jurisdictional exposure to government data access

CCIA Europe recognises the legitimate concerns that government and law enforcement data access laws raise among cloud customers and policymakers. At the same time, we are acutely aware of the pressing need to adapt law enforcement and intelligence communities' investigatory arsenal to a borderless digital age so that they can keep carrying out their duties and the public interests they pursue. CCIA believes that an intergovernmental solution should be pursued as a priority.

Extraterritorial government and data access laws are a global phenomenon which require multi-lateral safeguards. Unilateral measures such as those contemplated under the IIA risk pre-empting and potentially

[2] While EDPB guidelines are non-binding, they are used as a checklist by Supervisory Authorities during their investigation and their content is often reflected in national infringement decisions. Guidelines also remain important tools for companies in practice as they continuously seek to comply with their obligations.

[3] A summary of concerns that the EDPB guidelines on data portability has created can be found in CCIA Comments on the EC Data Strategy Consultation, May 2020, page 6, available on https://www.ccianet.org/wp-content/uploads/2020/06/FINAL-Supplementary-comments-CCIA-submission-on-EC-Data-Strategy-Consultation.pdf

conflicting with the outcome of on-going intergovernmental initiatives such as the 2nd protocol to the Budapest Convention, or the on-going OECD process on principles for government data access. With the Data Act, the European Union risks creating a conflict of laws and legal uncertainty for businesses.

In addition, before considering any one of the two unilateral policy options on non-personal data transfers and access, CCIA Europe invites the European Commission to thoroughly assess any evidence that would demonstrate the magnitude of the risk of foreign government access to EU non-personal data, including assessing the relevance of non-personal data for key national security and law enforcement purposes. The European Commission should also consider how each of the two options falls within the Article XIV GATS derogations and related jurisprudence.[4] Finally, we invite the European Commission to reflect on the significant trade-offs for economic actors in Europe. All the evidence shows that data transfer restrictions or otherwise similar measures "impose considerable costs on those forced to abide by [these requirements]."[5] 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,[6] and increase cybersecurity risks.[7] Overall, "stricter data policies have a negative and significant impact on the performance of downstream firms in sectors reliant on electronic data".[8] From a vendors' perspective, domestic data transfer restrictions "barring [or restricting] access to foreign services only invite reciprocal [measures] from one's trading partners",[9] and undermine local vendors' chances of exports.

Furthermore, EU norms to mitigate third-country government access to personal data are still maturing and many legal uncertainties remain unsolved at this stage, including what constitutes "reasonable legal, technical and organisational measures". They raise disproportionate requirements for companies to have in-depth knowledge of third country government data access laws and practices which routinely take years to complete in the context of European Commission adequacy decisions. Creating separate unilateral rules and a parallel enforcement framework for non-personal data could make it more complex to provide and procure services in Europe, and risk stifling the EU's objective to become a world-class data hub.

Finally, CCIA Europe cautions against establishing a unilateral adequacy-like mechanism such as described in the Inception Impact Assessment, similar to the framework under the 1995 Data Protection Directive and its successor, the GDPR. 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. This is why there are only 12

---

4 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

5 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

6 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;

7 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

8 *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/

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

adequacy decisions in place in the field of personal data protection, and only two of them cover the top 10 EU trade partners.

***

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