Computer & Communications Industry Association
Tech Advocacy Since 1972

CCIA Comments on the EC Data Strategy Consultation

May 2020

The Computer & Communications Industry Association (CCIA) welcomes the opportunity to provide comments on the European Strategy for Data.

Data-driven innovation is transforming Europe's economy and businesses across sectors use data to improve their competitiveness and offerings while public authorities can use data to better serve European citizens.

We agree with the European Commission that governments and regulators can help encourage voluntary data sharing practices where they demonstrably support social improvements and/or economic innovations and providing that they do not undermine data holders' rights and legitimate interests.

To that end, we offer our detailed comments on several aspects raised in the Data Strategy and the consultation survey thereof, namely:

EU investments in data technologies and infrastructures and the creation of common European data spaces (Section 1)

CCIA supports any efforts for companies and the public sector to create and reap the benefits of data-driven innovation in Europe. Investments in data technologies and infrastructures could be one way to do so.

However, these efforts can only be productive if they meet effective market demand. We recall that world class cloud services are already on offer in Europe and provide innovative data access and reuse solutions between authorised parties. It is essential that these investments do not deprive, directly or indirectly, European companies from these solutions, many of them leverage in-house or third-party technical means located in Europe and are subject to EU rules.

In our view, investment efforts should also be complemented by regulatory efforts to continue the good work the European Union has undertaken to ensure the free flow of data and remove unjustified and persisting barriers to cloud adoption. We address some of these in the following cloud computing section.

CCIA also welcomes efforts to facilitate access to open data in strategic industry sectors. CCIA has a long history of advocating for voluntary open data access that can positively impact the economy and society at large. But it is essential that participation in common European data spaces remain voluntary and non-discriminating.

We look forward to further contribute to this discussion in the coming months.

B2B data access and use and data governance mechanisms (Sections 1 and 2.1)

> ***Question:*** *One area of study are difficulties experienced in accessing and use data from other companies. With the following questions we seek to further examine the importance and the nature of data access issues in business-to-business situations.*
>
> *Have you had difficulties in using data from other companies?*

Voluntary B2B data access

The Data Strategy and the consultation survey refer to B2B data access and reuse and the governance mechanisms necessary to encourage data sharing between businesses.

CCIA could support measures to encourage voluntary data access if they are based on a "need-to-access" approach and providing that:

- data holders retain the freedom to choose the most suitable governance model to share data e.g. open data framework, licensing agreements or other types of contractual arrangements.
- data holders' rights are respected (e.g. IP rights, trade secrets, sui generis database right) and
- data access does not create conflicts with data holders' statutory obligations (e.g. data protection, security).

Any voluntary data access governance framework should also remain technology-neutral, and refrain from favouring one storage or access architecture over others.

CCIA would also caution against a voluntary data sharing governance framework solely based on FRAND terms as it is sometimes alluded to. Other governance frameworks may be better suited to the needs of the parties. For instance, open data schemes provide more generous conditions than FRAND terms for third parties to access data, including free-of-charge access and with little to no restrictions of use. Furthermore, 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. The European Union should generally refrain from inadvertently creating a regime where data is universally treated as an intellectual property, and where any innovation and research driven by text and data mining would require a licensing agreement.

Policymakers can help encourage B2B data access and further service interoperability where it makes sense, that is where and when there is a demonstrable business case, e.g. when demand for data exists and supply is low e.g. cybersecurity information sharing.

Mandatory B2B data access right / obligation

While this is not addressed in the consultation, the Data Strategy contemplates the introduction of a mandatory data access right under "fair, transparent, reasonable, proportionate and/or non-discriminatory conditions" and where a "market failure [in a given sector] is identified or can be foreseen, which competition law cannot solve."

CCIA disagrees with the introduction of a new statutory compulsory data access right/obligation.

In general, we believe that access to data is adequately addressed by existing legislation and enforcement. Furthermore, we caution against the long-term chilling effect that such a (sectoral) mandatory data access right/obligation would have on competition and innovation incentives, and the significant tensions it would create with data protection and privacy laws.

As the debate moves forward on this issue, several clarifications will be essential to help inform the discussion, including a clear identification of the policy objective(s) that this measure would pursue, to what extent existing laws and enforcement neither captures this objective nor provides sufficient remedies, and the type of data that would be subject to this new right/obligation.

Absent of any such clarifications, CCIA may only provide the following general statements:

(i) From a competition perspective, a mandatory data access right appears redundant at best. At worst, it would be harmful to innovation, competition, and consumer welfare.

CCIA agrees with the Commission that a data access right should only be sector-specific and only in circumstances where a market failure in the sector is identified which competition law cannot solve. CCIA submits that there are few circumstances where these conditions hold, and where the benefits of such mandatory data access outweigh negative side-effects on investment, innovation, competition, and consumer welfare.

First, competition law enforcement addresses agreements and restrictions that anticompetitively foreclose rivals. We recall that competition enforcers can already impose data access remedies where justified by market circumstances. Therefore, competition law can be presumed to resolve the vast majority of situations where data access is relevant.

Second, we can only presume that a mandatory data access right/obligation rests upon the assumption that access to said data is indispensable to compete on the market, that it is not available from other sources, that holders of such data are systemically and unjustifiably refusing to license said data, and that competition law enforcement cannot address the issue (otherwise lack of access would not amount to market failure). We question the validity of that assumption and the effects of mandatory access rights for two broad types of data:

- Raw and/or unstructured data: there are no reasons to compel access to this type of data since it is inherently non-rivalrous and widely attainable through other means. The use of raw, unstructured data does not reduce the amount of data available for others, and whatever access restrictions a given company has put in place for statutory or commercial reasons generally does not prevent others from collecting and processing the same data through other channels. The Commission has rightly recognised this in several acquisition cases involving various categories of data[1].

[1] See for instance M.7217 – Facebook/WhatsApp (3 October 2014), available here, §189: "there will continue to be a large amount of Internet user data that are valuable for advertising purposes and that are not within Facebook's exclusive control"; M.8124 – Microsoft/LinkedIn (6 December 2016), available here, §262: "there are many other possible sources of data which are already available for ML"; M.8180 - Verizon / Yahoo (21 December 2016), available here, §91: "the combination of the Parties' respective datasets will not raise the barriers to entry/expansion for other players in this space, as there will continue to be a large amount of internet user data that are valuable for advertising purposes and that are not within the Parties' exclusive control."

- Structured and/or inferred data: this type of data is the product of investments and is generally considered an intangible business asset. In some cases, it can also be the linchpin of an organisation's digital transformation. While some organisations may be keen to free ride on a competitor's investments, this data should not be considered necessary to compete on the market because it could be derived from the raw and/or unstructured data. Statutory mandatory access to structured and/or inferred data would effectively force organisations to share the fruits of their investments, be deprived of any incentives to process or innovate with data, and subsidise less innovative companies. CCIA cautions against the long-term chilling effect this policy would have on competition and innovation incentives.

Finally, compelling data access may also result in interoperability and data format mandates. While CCIA supports market-driven efforts towards interoperability, mandating interoperability across the board would be detrimental to service differentiation, competition, and consumer welfare. To name but one example, interoperability may require the use of common data formats across services. This would increase compliance costs for new entrants. Also, data formats have a direct implication on the diversity of the data which, in turn, may affect the diversity of services.

(ii) A B2B mandatory access right/obligation would run afoul of Europe's data protection law and undermine user control over their personal data

Even if introduction of a B2B mandatory access right were narrowly tailored to address a market failure-related purpose, it would necessarily create significant tensions with Europe's core data protection principles and the obligations and responsibilities of a service provider vis-a-vis their users.

Unlike the right to data portability under Article 20, we presume that a new compulsory B2B data access right would entail the transmission of datasets between two organisations without any individuals involved.

Given the broad definition of personal data, datasets may sometimes contain both personal and non-personal data that are inextricably linked and cannot be disentangled. In those instances, the introduction of a B2B mandatory access right/obligation would conflict with the core data minimisation, purpose limitation, security principles of the GDPR and the obligations and responsibilities of a service provider vis-a-vis the data subjects involved.

For decades now, the main purpose of Europe's data protection laws has been about empowering users and providing them with effective control over their data. The GDPR has significantly raised the bar in this respect.

The transmission of personal data from one service provider to third parties, and the subsequent processing by these third parties (be they competing or vertical service providers) for their own commercial purpose(s) would be subject to robust safeguards and limitations designed to put the user in control of his or her data.

For instance, the legal grounds available for competing or vertical service providers to process personal data acquired from a competitor would be severely limited. In all likelihood, competing or vertical service providers would only be able to obtain user consent[2], a high legal standard by all means, and difficult, if not impossible, to implement absent a direct relationship between the user involved and said providers (and if such direct relationship did exist, the justification to share such data on competition grounds would be limited). In addition, consent for the transmission of data to an infinite number of third parties would arguably be unlawful[3].

[2] 'Legitimate interest' of a third party involves several limitations, including the prohibition of further processing unless the original purpose of processing is 'compatible' with the subsequent processing. It is also limited to processing that a user can reasonably expect. 'Contract performance' necessarily requires a direct relationship with the user, and is limited to what is technically necessary to perform the service. 'Compliance with a legal obligation' would require proportionate and detailed statutory provisions regarding the purposes of the processing, categories of personal data involved, scope of the data subjects' right restrictions, safeguards to prevent abuse or unlawful access or transfer, storage periods, etc. (see Article 23(2) and Recital 45 GDPR).

[3] See revised EDPB guidelines on consent 05/2020 available on https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

The introduction of a B2B mandatory access right/obligation would also raise significant challenges to ensure that the transmission and subsequent processing by competing or vertical service providers meet the security requirements in Article 32 of the GDPR.

Data portability (Section 1)

> ***Question:*** *Do you think that it should be made easier for individuals to give access to existing data held about them, e.g. by online platform providers, car manufacturers, producers of wearables, voice assistants or smart home appliances, to new services providers of their choosing, in line with the GDPR?*

CCIA believes that data access and portability play an important role in how individuals control their data. Over the last few years, we observe more and more service providers rolling 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 suits their needs. As such, portability can facilitate competition among services and contribute to greater market innovation.

But data portability also involves several, sometimes conflicting, interests. On the one hand, data portability is one of the ways for individuals to control their data. However, exercising the right to data portability should not be detrimental to third party individuals' rights. Lastly, the right to data portability would serve no purpose if it is construed in abstract and without consideration to the practical and technical challenges it raises.

CCIA generally believes the General Data Protection Regulation ('GDPR') strikes the right balance between these considerations, and we strongly advise against upsetting this balance. However, **it would be easier for controllers to roll-out seamless portability functionalities if they had further clarification from the European Data Protection Board on some of the legal considerations set out in the box below**. In its 2017 guidelines, we note that the Article 29 Working Party suggests that the sending and receiving controllers must comply with several de facto requirements[4] to transmit and process data. **Some of these requirements are cumbersome, if not unrealistic** (let alone the fact that they seem to run afoul some of the core data protection principles) **and have a chilling effect for service providers willing to develop and deploy seamless portability solutions**.

Assuming the legal challenges are overcome, there are obvious technical challenges to the automated and seamless transfer of data from one service provider to another. 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[5]. All this has an impact on the system architectures of 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, (data) block by (data) block, and with user-friendliness always in mind.

[4] While 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.

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

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

Further clarification on certain aspects of the right to data portability under the GDPR

Data eligibility and third-party data: In its 2017 guidelines[6], the Article 29 Working Party suggests that the receiving controller must comply with several requirements to process third party data. These requirements can be cumbersome, sometimes unrealistic, and effectively prevent the portability of certain data, particularly third-party data. These requirements have a chilling effect for service providers willing to develop and implement seamless portability solutions for their users.

WP29 guidelines on the portability of third parties' data[7]	**Practical considerations and recommendations**
(1) The receiving service provider must identify and find another legal basis to process this data other than consent or contract.	The receiving controller must assess whether each piece of data contains third party data. If it does, the receiving controller must ensure that it has a legitimate interest to process the data assuming the conditions below are met. Since manual identification would require disproportionate resources for any service providers, the receiving controller is bound to automate this process. At present, the most sophisticated machine-learning technologies can still make mistakes even for the simplest datasets e.g. images. **Recommendation: The EDPB should clarify that this requirement and the complete fulfilment of a data portability request should remain a best effort obligation.**
(2) The receiving service provider must leave the data under the 'sole control' of the requesting user.	It is not clear how the requesting user can have 'sole control' over the data (s)he wishes to port to another service. Both the sending and receiving service providers are 'controllers' by all means. **Recommendation: We invite the EDPB to clarify or remove this section.**

[6] Article 29 Working Party guidelines on the right to data portability, 16/EN WP 242 rev.01 available on http://ec.europa.eu/newsroom/document.cfm?doc_id=44099

[7] Ibid. p.11-12

(3) The receiving service provider must process the data for the same purpose as the sending controller.	This requires the receiving service provider to have actual knowledge of the sending service providers' processing purpose(s). While controllers must inform users of the purpose(s) of processing under Article 13, this information may not be accessible publicly and may only be available when a user signs up to the service. As such, this would require that all sending and receiving controllers enter into an agreement to access each other's processing records. This would be very time-consuming for all parties into a potentially individual contract. In the unrealistic scenario where all providers would make this information public, it would be disproportionate to expect the receiving service provider to collect such information. **Recommendation: We invite the EDPB to reconsider this requirement. Until then, the EDPB should clarify once again that the complete fulfilment of a data portability request should remain a best effort obligation.**
(4) The receiving service provider must ensure that the requesting user manages the data for purely personal or household needs.	It would be disproportionate to expect the receiving service provider to check that each single user manages the transmitted third-party data for purely personal reasons or household needs. It would also conflict with the data minimisation and purpose limitation principles as it would compel the receiving service to process data that it would not otherwise need to perform the service. **Recommendation: We invite the EDPB to reconsider this requirement and ensure alignment with the data minimisation principle while encouraging service providers to develop and embed portability solutions within their respective service.**

(5) The receiving service provider must implement consent mechanisms for third parties involved.	This requirement also obliges service providers to process more data than they otherwise need to perform their service. To implement a consent form for third party individuals, the service provider must not only assess if there is the transmitted data contain third party data (as per (1) above) but also *identify* this third party in the event (s)he signs up to the service. The processing necessary for identification is arguably far more intrusive than the mere binary processing involved to match the transmitted data as belonging to the requesting user or someone else. Furthermore, developing such a consent form would compel service providers to dedicate unnecessary time and resources on the off chance that a pre-identified individual sign-up to the service. **Recommendation: We invite the EDPB to reconsider this requirement in line with the data minimisation principle while encouraging service providers to develop and embed portability solutions within their service.**

Active vs passive data

The Article 29 Working Party has broadly interpreted the right to data portability to include data observed (or 'passive') from activities of users such as raw data processed by a smart meter or other types of connected objects, activity logs, history of website usage or search activities — as opposed to data that the user has simply provided ('active' data).

In our view, this goes beyond the terms GDPR requires, and we share concerns expressed by the European Commission and stakeholders in that regard[8]. In practice, it is unclear why moving such data to another service would be at all beneficial for users.

Recommendation: we invite the EDPB to reconsider its position and align its revised guidance with the terms of the GDPR.

[8] 'European Commission, experts uneasy over WP29 data portability interpretation', IAPP, 25 April 2017 available on https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation-1/

Data literacy (Section 1)

> ***Question:*** *'General data literacy across the EU population is currently insufficient for everyone to benefit from data-driven innovation and to become more active agents in the data economy.' To what extent do you agree with this statement?*

CCIA agrees that data literacy among the EU workforce is generally insufficient. But data is only one component of the broader digital skills required for people to use, develop, and deploy digital innovations and make full use of the many options and choices available to them. In fact, CCIA believes the skills gap in coding and IT architecture has far greater consequences on the pace of digital transformation and innovations in Europe. Furthermore, CCIA believes that increasing Europeans' digital literacy in general will lead to a better functioning market for digital products and services.

Standardisation (Section 2.1)

The survey enquires about the role that the EU or national governments should take in field of interoperability standardisation.

CCIA believes that standardisation, in general, should remain a market-led process by all means. Market participants know what is needed. And while not all governments may have the necessary expertise required to be directly involved in defining standards, governments can raise general policy concerns that may be addressed by new standards and certifications.

In fact, experience shows that broader government policy considerations, whether they have been expressed through legislation, are oftentimes escalated in international standardisation consortia, regardless of whether governments have a seat at the table. For instance, ISO 27003:2019 was drafted and adopted with customers and governments' security perception in mind, and to provide a transparent and accountable framework for cloud service providers vis-a-vis their customers.

Specifically, on interoperability, we support the Commission's stewardship in convening global and European SaaS, PaaS and IaaS to produce the "SWIPO" Codes of Conduct.

Cloud computing (Section 2.3)

The consultation survey and the data strategy seek to identify "perceived risks" and "problems in the current functioning and constitution of the market for cloud services in Europe."

CCIA represents a broad range of cloud service providers operating in the EU. In our Members' experience, the lack of clear and up-to-date public procurement rules has led to a patchwork of undue national requirements that has reduced the availability of cloud service offerings and has inhibited the digital transformation of the public sector.

CCIA therefore supports the establishment of a "cloud rulebook" that compiles existing legislation and the development of common, non-discriminatory and open European cloud services marketplace and duly proportionate requirements for the public procurement of data processing services. In doing so, CCIA invites the Commission to consider the following principles:

- **Non-discrimination of cloud service providers:** The market should be open to all providers as long as they comply with European legislation, regardless of the location of its headquarters. EU cloud customers should continue to be free to select the providers and services of their choice.
- **Multi-tenancy:** Bespoke requirements excluding certain types of cloud services (e.g. the public cloud) should be prohibited in principle. Derogation to this principle should only be admissible if said requirements are duly justified and respond to objective and demonstrable needs or risks, and that they cannot be assuaged through technical or organisational risk-mitigation measures.
- **Shared responsibility:** While cloud service providers are responsible for protecting and maintain the integrity and continuity of the service, public sector customers remain responsible for the content and applications hosted on cloud services.
- **Contractual framework:** Terms of Service and Service-Level Agreements reflect service providers' expertise and deep understanding of how cloud services operate in practice and factoring in their constant technological evolution and innovation. Individually negotiated contracts can address customers' needs to the extent that they cater for shared services and facilities, which is a fundamental aspect of cloud ecosystems.

More generally, and beyond procurement, CCIA is concerned with:

- The increase of national standards and certifications which impede (1) market entry for non-domestic players and (2) market export for small domestic players
- Unjustified direct and indirect data localisation restrictions and discrimination on grounds of main establishment location.
- Misconceptions around the U.S. CLOUD Act generate concerns that negatively impact cloud adoption in Europe. For cloud customers to make risk-based decisions (and implement appropriate mitigation measures) supported on facts instead of perceptions, we encourage the Commission to raise awareness around government access to data in the cloud. An analysis of the rules and safeguards in this respect at the Member-States level, the U.S, and how those regimes interact with GDPR, international law, and the Budapest Convention would be helpful. We also strongly support the adoption of the EU-U.S. Agreement to facilitate cross-border access to electronic evidence for both parties, and ultimately provide certainty to the cloud market and boost innovation.

Finally, we recognise that there may perceived risks and that in practice, there is a fine line between prospective or existing customers' perception of the risks and real "problems". CCIA Members and the industry at large remain committed to assuage concerns through voluntary standardisation and certification. We also reiterate our support for the creation of a "Cloud Rulebook" to compile all applicable EU requirements and international industry-recognized standards to help existing and cloud customers identify measures to address objective risks.

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