Computer & Communications Industry Association
Tech Advocacy Since 1972

CCIA Response to the EU Finnish Presidency Consultation on the Data Economy Principles

October 29, 2019

Foreword

The Computer & Communications Industry Association (CCIA) welcomes the opportunity to comment on the draft principles prepared by the Finnish Presidency for a human-centric, thriving and balanced economy.

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 citizens.

We believe 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.

With that mind, we respectfully submit our comments on the draft data principles put forward by the EU Finnish Presidency.

1. Access

Access by default. Access to data according to various access rights (e.g. business-to-business, business-to-government) should be facilitated by technical or legal solutions and support.

Access to the necessary data of each sector for various purposes should be provided on fair, reasonable and non-discriminatory terms while respecting rights of individuals and businesses.

Data must be digital in machine-readable format, and if possible available as real-time data. Access to data is provided and controlled through an open programming interface (API) within the entity that provides the data.

Once-only principle. Data should be stored only once to enable easy access and timeliness of the data.

Publicly funded data sets should be open data and provided through open interfaces for individuals and businesses by default.

How important is this?	3/5	Is it feasible?	No

General comments

"Access by default" implies that all kinds of data held by any authorities, companies or individuals can be accessed by anyone, be they individuals, business competitors, governments and private third parties.

CCIA disagrees with this approach and recommend that access should be encouraged on a "need-to-access" basis, providing that:

(i) 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,

(ii) data holders' rights are respected, and

(iii) data access does not create conflicts with data holders' statutory obligations.

We recall that some data may be protected by IP rights and should not be accessible by third parties, particularly when a dataset is the result of in-house investment (e.g. where the data constitute inferred conclusions from algorithmic processing) or pertains to trade secrets or protected under the Database Directive (e.g. manual or automated collection of prospective customers, or airlines' flight routes technical and passenger capacity data).

FRAND terms

Data holders should enjoy the freedom to choose the most suitable governance model to share data. The use of FRAND terms should not be the only way to provide access to data. 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, '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.

Characters of the data

CCIA agrees that data, including real-time data where relevant and possible, should be supplied in digital form and in machine-readable format. However, any data access principle should remain technology-neutral, and refrain from favouring one technology (e.g. API) over the others (e.g. screen-scrapping, File Transfer Protocol (FTP) services, controlled access to Online data repositories/portals or industrial data platforms, etc.).

'Once-only' data storage principle

The assumption that shared data should be stored only once implies the centralization of data providing third parties restricted and remote-only access. While this may be appropriate in some instances and fits the description of some technologies, it may not be suitable for others e.g. blockchain, data downloads, etc. In other words, data storage, and the occurrence thereof, depends on the technology and general framework used to provide access to those data.

2. Share

Reusable by default. Data sets need to be interoperable and harmonised in a structured format to enable flow of data in automated processes.

All new initiatives for the production, collection and processing of data should be based on the principle of interoperability and in mutual reciprocity.

Reusability should be supported by interoperability measures such as

- open standards and structured data sets
- commonly used technologies and information systems
- codes of conduct and model contractual agreements
- governance structures for data exchange and value sharing in ecosystems.

Restrictions on data sharing should be based on well-defined reasoning at the corporate policy level and should not restrict third-party value creation.

Conditions for data sharing that is justified by a clear and demonstrable public interest need to be established. Public bodies should ensure that their request for the reuse of private data are balanced (e.g. proportionality, functioning markets).

How important is this?	3/5	Is it feasible?	No

General comments

CCIA supports efforts to encourage open standards and codes of conduct to foster interoperability across digital services. Interoperability is essential for the free flow of information across Europe's economy. Fostering interoperability across relevant services can help boost competition and improve existing or new products in separate vertical markets.

That said, not all services should be made interoperable, and not all data should be made portable across all services. Service interoperability may be useful for users to migrate data between relevant services, whether it is to switch providers or complement users' technology stacks. However, it is unclear why service providers operating in vastly different markets should make their services interoperable. Interoperability should be encouraged where there is a demonstrable business case.

Secondly, mandating interoperability across the board would be detrimental to service differentiation, competition, and customer welfare. We recall that interoperability may require the use of common data formats across services. Formats have a direct implication on the quality of the data which, in turn, may affect the quality of services. By way of analogy, consider differences of image formats between JPEG, a lossy data format with suboptimal compression rate popular for easy viewing,

file transferring and storage, and TIFF (Tagged Image File Format), a lossless format used for graphic designs because of its flexible compression quality without deprecating image color and information. The better the quality of the data, the more likely it can meet sophisticated graphic design software capabilities. Encouraging the development of common data formats where they are needed is helpful, but we caution against mandating common data formats that would impoverish product innovation and reduce customer choice.

Motives driving interoperability

Policy-makers can help encourage further interoperability where it makes sense, that is where and when there is a demonstrated business case, e.g. when demand for data exists and supply is low e.g. cybersecurity information sharing.

CCIA does not believe that "public interest" – an arguably vague and volatile concept - should be the only motive that drives policymakers' efforts to promote interoperability. Efforts to promote interoperability should be focused, pragmatic and in tune with market trends, rather than general and conceived in abstracto. Policymakers can accompany industry-led interoperability efforts This is for example the case with the on-going drafting of EU Codes of Conduct on Cloud Switching ('SWIPO').

Consideration to third-party value creation should not be the primary motive for a private sector organisation to make data interoperable. In some cases, data sharing/from third parties may be an integral and sometimes indispensable part of a wide variety of products[1]. In other cases, data may be commercially sensitive and treated as an intangible business asset. Providing such data to third parties would be highly inadequate.

3. Act

Human-centric by default. Individuals are guaranteed access to their personal data and means to manage the reuse of their data without lock-ins or impediments that inhibit access or portability (e.g. timeliness).

Users should be given full control and portability of their data, while safeguarding privacy.

Transparency and clear terms and conditions to understand how their personal data is used in services and automated decision-making (also by third-parties).

Empowering individuals to manage their data rights requires easy to use tools

- to manage access to and the reuse of their data (e.g consents)
- to increase findability and reusability of user-generated contents (e.g metadata)
- to change service provider (e.g relocate data)

How important is this?	3/5	Is it feasible?	Yes

[1] See for instance Red Hat OpenStack Platform, McAfee MVISION, online payments system such as Stripe

CCIA supports a meaningful and pragmatic implementation of all data subjects' rights under the General Data Protection Regulation.

However, we do caution against the assumption that consent is an "easy (...) tool (...) for users to manage access to and reuse of their data". Consent remains a high legal standard[2] and, to quote the UK data protection authority, "consent won't always be the most appropriate or easiest."[3] In the context of GDPR, consent is isolated to situations where no other lawful bases apply. Data protection authorities have recommended that consent may not be the most suitable ground of processing in many instances and the choice of the lawful basis should most closely reflects the true nature of an organisation's relationship with individuals and the purpose of the processing[4]. We recall that user control and transparency over personal data processing are addressed in several chapters and provisions of the GDPR – including the right to information, access, rectification, erasure, and portability, the right to object to processing, and the right not to be subject to automated decision-making, along with the necessary obligations for controllers and processors to give effect to user rights.

4. Innovate

Level-playing field by default. Data market access should be open to all on fair and non-discriminatory basis for the benefit of everyone. Undistorted competition in data markets should be guaranteed.

In order to enable innovations, the findability of data and data reusability should be supported by

- data catalogues, extranets and other published channels
- commonly accepted data models, standards, ontologies, libraries and schemas
- functioning licensing
- mechanisms for balanced value sharing

How important is this?	3/5	Is it feasible?	No

See our comments on the access by default and reusable by default.

[2] According to the EDPB, consent is deemed valid if users make a deliberate and free choice to actively accept a specific processing operation (no opt-out) and if they have been "adequately" informed about the purpose of a given processing operation and their right to withdraw consent. Some DPAs have also argued that free consent should also mean that the absence of consent should not be detrimental to the users, and services should still be provided.

[2] See the ICO guidelines on consent

[2] See for instance EDPB guidelines on consent or CNIL guidelines on consent.

Computer & Communications Industry Association
Tech Advocacy Since 1972

5. Trust

Ethically sustainable by default. Building trust in data use and data-driven technologies requires strong respect for human rights, and transparency, reliability and the inclusion of all stakeholders. Data security and privacy by design should be integral parts of business and service development practices.

Trust is created and maintained by

- clear responsibilities for data management
- easily understandable digital services and products
- transparency (e.g. traceability, explainability, interpretability) of algorithms as well as autonomous and intelligent systems
- traceability (e.g. logs) and security when processing data throughout data lifecycles
- use of new technologies and mechanisms that build trust in decentralised data-sharing networks (e.g. blockchain)
- establishment of accountability for intended and unintended consequences of gathering, processing and using data

How important is this?	4/5	Is it feasible?	Yes

CCIA agrees with all of the points above.

We believe that the level transparency and the granularity of the explanation of an algorithmic decision should be depend on the general application of a given product and the intended audience of this product.

As far as B2C products, we believe that the relevant information should generally be disclosed in intelligible and plain language.

We recognize that additional information may be needed for B2B and B2G products depending on the purpose(s) and application of algorithmic decisions. The level of granularity should be left to the discretion of the contractual parties, on a case-by-case basis.

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

CCIA Europe • First Floor • Rue de la Loi 227 • B – 1040 Brussels, Belgium • 32-2-888-8462