ECIS European Committee for Interoperable Systems

ECIS ivzw-aisbl
Louizalaan 65 avenue Louise Box 2
B-1050 Brussels, Belgium

T/F +32 (0)2 706 24 15
info@ecis.eu
www.ecis.eu

13 September 2022

ECIS POSITION PAPER

ON THE EUROPEAN COMMISSION DATA ACT PROPOSAL

1. BACKGROUND ON ECIS

The European Committee for Interoperable Systems ("**ECIS**") is an international, non-profit association of information technology companies founded in 1989 which endeavours to promote a favourable environment for interoperable ICT solutions. For three decades ECIS has actively represented its members on issues relating to interoperability and competition before European, international, and national fora, including the EU institutions and WIPO. ECIS' members include both large and small information and communications technology hardware and software providers, including IBM, McAfee, Opera, Oracle, and Red Hat. For further information, please see ECIS' website at www.ecis.eu.

2. FEEDBACK ON THE PROPOSAL FOR THE DATA ACT

At the outset of this position paper ECIS would like to emphasise that the Data Act Proposal (hereafter "**Data Act**" or "**Proposal**") is a timely, welcome and useful legislative proposal that will contribute to the European Commission's ("**Commission**") strategy for data, aiming to ensure a fairer, more open, and transparent approach towards data flows. With this paper, ECIS, having 30 years of history striving for better system interoperability, both in terms of software and data, intends to build upon a previous position paper published in support of the Commission's overarching information society goals.[1]

ECIS looks forward to sharing its technical and policy insights with the Commission in a constructive dialogue. As currently drafted, especially on switching and interoperability, the

[1] http://www.ecis.eu/wp-content/uploads/2022/05/ECIS-feedback-on-the-European-Commission-proposal-for-the-Data-Act.pdf

proposal runs the risk of falling short of expectations by using broad brush measures and not providing a sufficient level of detail on how provisions will work in practice. The proposal should be mindful of not inadvertently interrupting those existing market arrangements and practices that promote innovation, interoperability and portability. Therefore, ECIS believes that the proposal can be improved by making it more targeted and precise.

Chapter 2 – Protection of trade secrets

The Data Act provisions on IoT data sharing as currently drafted risk hampering innovation by obliging the transfer of data sets that may contain trade secrets. The protection of trade secrets (and related intellectual property rights or other proprietary rights) often provides both a differentiator and additional incentive to continuously innovate. Data sets themselves can represent significant investment in terms of software development, data processing, storage and privacy/security protections. Therefore, companies should never be forced to share trade secrets and intellectual property with third parties. Trade secrets should, as a matter of principle, be excluded from any data sharing obligation.

Chapter 6 – Protection of trade secrets and intellectual property

Similarly, the provisions on data portability in Chapter 6, also risk capturing a data set that is too broad, thereby hampering innovation and important differentiator incentives. According to Art. 23.1(c) Data Act, data processing service providers must enable the portability of all "*data, applications and other digital assets.*" Such an obligation is overly broad and will not, we believe, contribute towards the ambitions of the Proposal. Forcing the incumbent service provider to enable the porting of *all* above-mentioned data to a receiving service provider, without sufficient trade secret protections, runs the risk of service providers not sufficiently investing and thereby impeding much needed innovation across European data spaces.

Chapters 6 & 8 – Hybrid cloud complexities and realistic porting, switching and interoperability

The Commission's Data Act provisions related to cloud switching and interoperability seem to presuppose and/or support a view that all software and data in the future is homogeneous and will run on public cloud infrastructures. In fact, cloud is heterogeneous and deployment modes such as hybrid cloud computing and a multi-cloud approach will continue to play a crucial role. ECIS has on multiple occasions written about the importance of Hybrid cloud[2] and the implications this has on data portability and interoperability.[3] For the avoidance of doubt, hybrid cloud is generally understood as a cloud service delivery that uses at least two different cloud deployment models whereby a deployment model refers to the way in which cloud computing can be organised based on the control and sharing of physical or virtual resources, including public, private and community clouds.

[2] http://www.ecis.eu/wp-content/uploads/2010/10/ECIS-Hybrid-Cloud-Paper.pdf

[3] https://www.ecis.eu/2016/06/special-paper-on-cloud-computing-portability-and-interoperability/

Disadvantages of public clouds are that the customer cedes control over the physical resources involved, and since the resources are shared with other cloud service customers the potential for variable performance or data leakage across multi-tenant systems may exist. Hence not every IT solution is suited to using resources that are not directly controlled or managed. Therefore, enterprises will still require some level of private resources to meet their needs. Depending on user requirements such as higher levels of resilience against cyber-attacks, data residency or latency for example, cloud services may be based on specific hardware architectures or software assets. For example, banking systems require a high level of cybersecurity and operational resilience. An overly broad approach to cloud data porting and switching could in such circumstances create undesired dangers. Moreover, specifically for financial services, the Commission has proposed the Digital Operational Resiliency Act ("**DORA**"), containing provisions on effective switching to other ICT service providers. Taking initiatives such as DORA into account, which are sector specific and precisely defined, the broad horizontal scope of the Data Act proposal seems inappropriate.

Hybrid cloud solutions in today's market are irreplaceable, they offer great agility, flexibility and value in facilitating an approach to cloud deployment which fits the business model and business sector. However, hybrid cloud solutions also rely on the ability to bridge between different data sets and cloud services whether they be on-premise (in-house) or in the public cloud. As a result, portability and interoperability are vital. Because of the reality of hybrid cloud solutions, it is critical to understand that portability of data is not simply a "true or false" metric. There is a spectrum for data portability that can require a variable amount of effort, cost and risk to enable. The level of portability (as a measurement) can be defined as the amount of effort required to move from one system to another, depending on the source. This level will be dependent on factors such as the data format of the source and destination cloud service, but also the content and semantics – whether the data has the same meaning in the source and destination cloud service – of the data. The technical and operational challenges of switching cloud services and porting data need to be taken into account in the EC's policies. Even for open source solutions, portability is not necessarily a straightforward exercise, as software layers such as operating systems evolve or may be customized in specific use cases, although ECIS believes that the use of open source software significantly aids cloud interoperability. ECIS encourages and supports the EC's recognition of the importance of open source in this context.

Chapters 6 & 8 – Functional equivalence

In ECIS' view, the references to "functional equivalence" in the Data Act Proposal (contained in Chapters six and eight) require further clarification and explanation on how this should work in practice. As set out above, the ability to port data is determined by the format and content expected and supported by the source and destination system. These elements are influenced by the data storage system, the infrastructure deployed and software that interacts with the data. In certain instances, data is closely related – or even purposefully designed – to function with the hardware and software that process the data. Taking into account such tailor made solutions, the requirement of "functional equivalence" in data portability appears not only excessively burdensome but technically unfeasible. For example, a cloud service provider might develop a tailor made solution

to work with a certain operating system. The language in the Data Act proposal on functional equivalence seems to require, even under such circumstances, that the source cloud service provider should ensure a "minimal level of functionality." In other words, even if the destination cloud service provider does not have the required hardware or software architecture to ensure functionality, in essence, the data act would require the source cloud service provider to ensure portability and functionality adapted to the design of the destination cloud service provider's software. Establishing such an onerous duty upon the source cloud service provider, whereby it is essentially required to hand over (and adapt) the fruits of its own labour with its intellectual property seems neither desirable nor conducive to innovation or competition.

Moreover, Art. 26 Data Act as it is currently drafted seems to require that the source cloud service provider continues to ensure that the customer enjoys functional equivalence after a switch to a new cloud service. This wording goes against what is set out in recital 74 of the Data Act. First of all, recital 74 Data Act explains that data processing service providers should not be required to ensure functional equivalence in an environment other than their own. Secondly, it is set out that service providers are required to offer all assistance and support that is required to make the switching process effective, indicating that any obligation of ensuring functional equivalence on a source cloud service provider should be limited in time to the duration of the switching process.

In any case, functional equivalence is defined as "*the maintenance of a minimum level of functionality in the environment of a new data processing service after the switching process, to such an extent that, in response to an input action by the user on core elements of the service, the destination service will deliver the same output at the same performance and with the same level of security, operational resilience and quality of service as the originating service at the time of termination of the contract.*" By definition; the requirement to maintain a minimum level of functionality requires for each sector or vertical involved, either through the individual agreement with the customer or another more broadly supported consensus, to establish and define exactly what elements constitute core elements.

Chapter 6 – Switching costs

ECIS strongly supports the need for efficient data portability in cloud services. However, as pointed out above, portability is far from straightforward in most instances, depending on factors such as the architecture and functionality of the source and destination cloud service provider, but also on the amount of data to be ported. Therefore, in order to make the transition process efficient and cost effective, data portability requires collaboration between both service providers. Because of this need for collaboration between the source and destination cloud service provider, and the sometimes very costly switching process, a rigid obligation on the source cloud service provider to carry all costs involved with cloud data portability, runs risks of leading to abuses and hampering efficient switching. At the very least, some level of flexibility concerning the costs involved is desirable, such as ensuring that switching costs would be transparent from the outset of the contract.

Chapters 6 & 8 – Gatekeepers

The Digital Markets Act ("**DMA**") aims to redress inefficiencies and imbalances in digital markets, including the market for cloud services. Under the DMA, the Commission is allowed to designate a provider of a core platform service as a "gatekeeper." The DMA imposes a number of obligations on such designated gatekeepers, including an obligation to ensure effective rights to data portability.

In Chapter 2 of the Data Act proposal, it is established that gatekeepers, given the unrivalled ability of these companies to acquire data, would not be able to benefit from the data access right to Internet of Things ("**IoT**") data. According to the Commission, an access right for gatekeepers would not be necessary to achieve the objective of the Data Act. Following the same logic, and with the aim of ensuring a competitive cloud services market, ECIS is of the opinion that far reaching obligations set out in Chapter 6 and 8 of the Data Act, such as maintaining functional equivalence and a complete withdrawal of switching charges, should also be limited to those cloud service providers designated as a gatekeeper under the DMA.

***