Joint Industry Statement on the EU Data Act

May 11, 2023

In the context of the ongoing inter-institutional ("Trilogues") negotiations on the EU Data Act, the signatories, representing leading organizations in the technology, security and innovation sectors, highlight here key improvements in the Council's and EU Parliament's respective positions, and raise remaining concerns that are critical for Europe's innovative strength and competitiveness.

I. B2B data sharing (Chapters II & III): Protection of intellectual property and trade secrets

We support the EU Commission's objective to develop and increase data sharing and re-use (Chapters II and III), but we are concerned with implications for intellectual property and particularly trade secrets resulting from mandatory data sharing obligations.

In that regard, the changes made by the European Parliament (EP) and the EU Council address many of the concerns. Specifically, we support **the European Parliament's clarification of the "data holder" definition** laid out in Article 2.6 **with** the **mention** of the **"contractually agreed right to use such data".** We also support the **introduction,** by both co-legislators, **of further mechanisms to protect companies' trade secrets** (EP's Article 5.8 and Council's Article 4.3a), as well as the possibility for the data holder to refuse data access requests under exceptional circumstances.

We urge the co-legislators to ensure that the final version of the Data Act does not include obligations that would require sharing of intellectual property and trade secrets. This would be a clear contradiction with the 2016 Trade Secrets Directive and mandatory data sharing would infringe on cloud service providers' (CSPs) contractual agreements with their customers, specifically those preventing the sharing of such data without the customer's knowledge and consent.

II. Cloud switching (Chapter VI): Ensure diverse, secure, cost-efficient and state-of-the art solutions with feasible requirements

We **support the principle of "cloud switching"** (Chapter VI) and we welcome measures to facilitate it, as data portability is increasingly expected by customers and cloud users.

In that regard, we **welcome** the **key improvements** made by the co-legislators such as the good faith obligations (Article 24b of the EP text), the exclusion of the PaaS and SaaS delivery models from unfeasible "functional equivalence" provisions (Recitals 72 in EP & Council texts), the cooperation between the origin and destination CSPs and the customer/user which better reflects the various roles and responsibilities in such processes, and the exemptions and protections for trade secrets.

However, **concerns remain as to the practical implications of the provisions of Chapter VI.** We believe that the new switching requirements should be proportionate and feasible (CSPs cannot be held responsible for the aspects of switching they do not control), take into consideration the elements which are under the customer's sole control, and should increase, rather than restrict, European customers' access to diverse, cost-efficient and state-of-the-art solutions.

In particular, the **concept of "functional equivalence"**, as introduced by the EU Commission, **is problematic.** It would hold CSPs responsible for ensuring 'functional equivalent' experiences (extending to the same quality of service and cybersecurity) in their competitor's environments. The CSP cannot access their competitor's environment to ensure that equivalence, for obvious cybersecurity, intellectual property, trade secrets and competition reasons.

Moreover, while we recognize the Commission's objective to address vendor lock-in, it cannot be done through disproportionate impediments to the Business-to-Business (**B2B**) **principle of contractual freedom**. The contracting parties are best placed to determine whether a **contract takes into consideration** their **interests** and **the complexity/volume of their data sets as well as determining the right price**, based on those criteria. Therefore, they must remain allowed, via their contractual agreement, to determine alternative notice periods and termination rights, e.g. leveraging beneficial fixed-term contracts. Indeed, **fixed-term contracts** are the most used contractual models in B2B contexts as parties normally rely on multi-year commitments reflecting long deployment timelines, front-loaded implementation costs, price reductions, and other factors. More importantly, they are **beneficial to both parties** as they increase predictability for cloud service providers which is most important, in particular, for CSPs that are SMEs[1] while allowing business customers to enjoy a lower subscription price. In that regard, we support the Council's new Recital 72b[2], as well as the European Parliament's addition to Article 23(1)(a)[3].

Finally, the **switching** of CSP **should not involve sharing of security-sensitive data with customers**, as it cannot only lead to security risks to the product but also to the related services and to the user itself. The Act should contain provisions that recognise the obligations of the data holder to maintain the security of the processing when transferring the data.

III. Interoperability (Chapter VIII): Ensuring compatibility with international commitments

We are also concerned that the European Commission's proposed approach on **interoperability** (Chapter VIII), rather than facilitating switching, could **reduce choice for enterprise (B2B) customers in Europe**, lead **to less innovative features on offer,** and **potentially conflict with international IP (TRIPS) commitments**.

Regarding the latter, **Chapters VI and VIII** of the Act create obligations on data processing services to enable "functional equivalence" which will **impact Member States' ability to fulfil their international obligations under the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights** (**TRIPS**[4]). Where a data processing service provider owns intellectual property covering its services, any requirement to implement a "functionally equivalent" service will require the originating service

[1] SMEs are expressly protected by the Data Act against unfair contractual terms, with regards switching, in Article 13, paragraph 4, point e).
[2] The mention that "*nothing in the Data Act prevents (…) parties from agreeing on contracts for data processing services of a fixed duration, including termination charges to cover the early termination of said contracts, in accordance with national and Union law*"
[3] It allows for "*an alternative notice period [that] is mutually and explicitly agreed between a customer and a provider*.".
[4] The international agreement which sets minimum standards for intellectual property rights among WTO member states.

provider to license their intellectual property, or that of a third party, to the destination service provider. This is in direct conflict with TRIPS[5].

***

In **conclusion**, we urge the EU policy-makers to address these concerns of utmost importance for the technology, security and innovation sectors concerned, their customers and users, as well as Europe's innovation and competitiveness, namely: protection of IP and trade secrets in the B2B chapters, ensure diverse, secure, cost-efficient and state-of-the art solutions with feasible requirements for the cloud switching Chapter, and ensure compatibility with international commitments with regards the interoperability provisions.

Signatories:

AFNUM – The French Alliance of Digital Industries

BSA | The Software Alliance

eco – Association of the Internet Industry

Euralarm – Association of the electronic fire safety, extinguishing and security industry

ITI – Information Technology Industry Council

SCOPE Europe - Self and Co-Regulation for an Optimized Policy Environment in Europe

[5] These obligations notably include: Article 41 requiring members to enable effective enforcement action against any act of infringement of IPRs; Article 28 ensuring the patent owners' right to conclude licensing contracts; furthermore, the conditions for compulsory licensing under Article 31 are not met. A concrete example of such impact on TRIPS is as follows: Switching with the aim of preserving functionality directly impacts the proprietary innovation layers of products and services, where research and development investment is focused, and proprietary intellectual property rights are sought. For example, consider innovation at the IaaS layer - Research and development at this layer includes methods for maintaining quality of service, such as innovative methods of providing failover, load balancing and maintaining service speeds. Even at the IaaS layer, such functionality is heavily protected by intellectual property rights. Requirements to make interfaces open which are subject to patent protection in order to facilitate switching or interoperability is another example of how intellectual property rights are impacted by the obligations set out in this regulation. Requirements relating to platform and service layers higher up the technology stack that are even richer in features will impact an even greater volume of intellectual property rights.