EU Data Act:
Joint Industry Concerns About
Data Flow and Cloud Restrictions

15th June 2023, Brussels

We, the undersigned associations, representing both cloud customers and cloud vendors in the European Digital Single Market, are deeply concerned about the upcoming restrictions on data flows and cloud services as foreseen in Article 27 of the proposed Data Act. Our members – which include SMEs, start-ups, and large enterprises – rely on first-class, scalable digital technologies in order to provide their services and products across the EU and beyond. They work tirelessly to build a competitive, innovative and resilient digital economy in Europe. That is why it is so worrisome to see that the new restrictions on data flows and cloud services in the Data Act risks undermining our sector's efforts in achieving the EU's ambitious 2030 Digital Targets.[1]

First, the Data Act may conflict with data transfer rules under Chapter V of the General Data Protection Regulation (GDPR). In practice, cloud providers do not know the content of customers' data and are unable to identify whether the data they process on behalf of their customers constitute personal data or non-personal data,[2] let alone to provide separate processing infrastructure for each of those datasets. In addition, legal requests do not typically target non-personal data only. By creating a parallel – yet different – regime for the transfer of non-personal data outside the EU, Article 27(1), if unchanged, may lead to cloud providers being prohibited from transferring personal data to a third country even though it provides an "adequate" level of data protection status. In practice, this would render "adequacy decisions" and any other GDPR data transfer rules null and void.

Furthermore, we are concerned that Article 27(1) will lead to the development of "immunity requirements" against non-EU cloud providers and disproportionate obligations for European cloud providers with global operations. The open-ended nature of this obligation[3] lays the groundwork for the design and implementation of blunt discriminatory requirements against any cloud provider subject to foreign laws, be it in the forthcoming EU Cybersecurity Certification for Cloud services,[4] or elsewhere.

---

[1] See Article 4 of Decision (EU) 2022/2481 establishing the Digital Decade Policy Programme 2030, available on https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022D2481

[2] In addition, note that according to a recent General Court decision, the same dataset may constitute "personal data" or "non-personal data," depending on the context of processing, which makes the identification process even more challenging. See GC ruling in T-557/20, SRB v EDPS available on https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62020TJ0557

[3] The essence of Article 27(1) is a general obligation for cloud providers to take measures and demonstrate that they are effectively immune to conflicting foreign extraterritorial laws. In practice, we stress that companies are not in a position to identify potential conflicts of laws since it would require a comparative constitutional and legal analysis between third country government data access laws on the one hand, and EU or national laws such as IP, trade secrets, and "the fundamental interests of a Member State related to national security or defense".

[4] A leaked version of the EUCS scheme explicitly refers to the "immunity requirements" of EUCS in Annex J as a way to demonstrate compliance with Article 27 of the Data Act.

Finally, the lack of protection for trade secrets in Articles 4(3), 4(3a), 4(4), 5(8), 5(8a), 6(2)(e) and Recital 28a is likely to hinder companies operating in Europe. The nature of the trade secret protections is that they can be kept secret. This is exacerbated by a very narrow non-compete clause (only for development of directly competing products to the product from which data originates). While we appreciate attempts to set out scenarios under which trade secrets need not be disclosed, the requirement to identify and justify trade secrets is likely to make this of limited practical benefit. The data holder should be able to refuse access to data that consists of trade secrets.

To ensure the continued growth of the European digital ecosystem and to provide first-class digital technologies to customers in the EU and beyond:

- We urge the Data Act negotiators to recognise cloud providers' adherence with GDPR provisions for the transfer of personal data as fulfilling the requirements of Article 27(1) of Data Act for transfer of non-personal data.

- We invite Council and Parliament negotiators to adopt clear and pragmatic obligations for European cloud providers operating internationally and global cloud providers operating in Europe.

- We invite negotiators to avoid foreclosing any future political, evidence-based debate which several Member States and MEPs have requested[5] before adopting blunt discriminatory requirements. Because these may reduce Europe's cloud computing capacity, lead to fragmentation of the EU Digital Single Market, increase cybersecurity risks, and break international trade rules.

- We call on the European Commission to abandon unilateral, disproportionate measures in the Data Act and subsequent legislation. Instead, it should address demonstrated and legitimate concerns about extraterritorial government access to EU non-personal data. This should be done separately, strategically, and constructively with like-minded security and commercial partners — consistent with the EU's recent commitment to the *Data Free Flow with Trust* initiative of the G7.[6]

[5] See statements from Germany, Denmark, Estonia, Greece, Ireland, Netherlands, Poland and Sweden, among others, as reported by Euractiv: https://www.euractiv.com/section/cybersecurity/news/germany-calls-for-political-discussion-on-eus-cloud-certification-scheme/

[6] G7 Ministerial Declaration following Digital and Tech Ministers' Meeting on 30 April 2023 available on https://g7digital-tech-2023.go.jp/topics/pdf/pdf_20230430/ministerial_declaration_dtmm.pdf

Signatories:

INFOBALT

Digital Poland Association

Computer & Communications Industry Association – CCIA

Slovak Alliance for Innovation Economy – SAPIE

Digital National Alliance Bulgaria

Association of the Internet Industry – eco

The Information Technology Industry Council – ITI

Spanish Association of Digital Economy – adigital

Association For Applied Research in IT – AAVIT

Employers' Association of the Software and Services Industry – ANIS

DOT Europe

Union of Entrepreneurs and Employers - ZPP