DOT Europe position paper

Data Act

Portability of cogenerated data

DOT Europe supports empowering users to access cogenerated data but is concerned that the portability provisions as proposed risk undermining competition, cybersecurity, intellectual property and privacy, and reducing trust in the data sharing ecosystem. The provisions would also carry a high cost of compliance – for example requiring manufacturers to provide access to data that is encrypted and stored locally would in some cases imply a complete 're-engineering' of the product. In addition, giving users the ability to manage data generated by their devices could lead bad actors to access it. In the case of diagnostics data this could be used for purposes the users are not aware of, or to hack the device.

Finally, preventing users from sharing data under Article 4 with companies that provide core platform services and have been designated as gatekeepers under the DMA is arbitrary and undermines the overall objective of empowering users to access and share cogenerated data with third parties of their choice. It is in the user's and wider ecosystem's interest to be able to freely choose a data recipient.

Recommendations

DOT Europe would propose providing **more robust safeguards for trade secrets, competition and IP** to avoid undermining investments in innovation. Trade secrets protections should not differ depending on whether a user (which could be a business) or a third party is at the receiving end, or whether trade secrets relate to a product or a related service. Robust trade secrets protection should also be provided where a government shares with third parties any data it acquires from a service provider. References to the Trade Secrets Directive should be included throughout and severe consequences (not just judicial recourse) should be provided for any data recipients in the event of unauthorised disclosure of trade secrets.

We would also suggest restricting provisions to data where **the manufacturer or provider of a related service has some ability to get access or identify the data** and not e.g. where the data is locally stored on the device. More clarity should also be provided on what is "good commercial practice in data access and use" and what constitutes FRAND terms in the context of data-sharing obligations.

Finally, we recommend **removing the links to the DMA gatekeeper regime** and allowing users to port their data to products and related services of their choosing. If the DMA designates a data holder as a gatekeeper, then there are regulatory obligations that kick in and competition law is still available to impose behavioural remedies to the extent the gatekeeper is found to be dominant and to abuse its market position. We would also flag that excluding not just the provider, but the entire undertaking to which the provider belongs, from the possibility of being a data recipient is excessive, especially when these are providers with a proven track record of developing products and services that consumers value and that benefit SMEs. We would also point out that users may be more willing to

Rue du Trône, 60, 1050
Brussels, Belgium
Tel: +32 (0) 472 26 83 02

WWW.DOTEUROPE.EU
Transparency Register: 53905947933-43
DOT Europe was formerly known as EDiMA

try new products and related services by porting the data to new entrants in the space, if they are aware they have the possibility to go back to the original service provider in case they are not satisfied with the new products and related services used.

B2B data contracts

DOT Europe would question the need for detailed provisions in this area given that the B2B data industry is thriving in the EU and unequal bargaining power is a common feature in many markets which does not in itself constitute a market failure. The Data Act should not disrupt existing B2B data sharing models, but rather aim to provide European businesses with the ability to choose among the widest range of data sharing mechanisms and contractual models that exist in the market, as different use scenarios may require different features (level of protection, access restrictions, etc.). Also, under Chapter IV the data holder bears the burden of proving that the contract terms were not unilaterally imposed, creating a presumption that is almost impossible to overturn.

Recommendations

While we understand the intended beneficiaries of these provisions are MSMEs, we believe the appropriate means to achieve the proposal's objectives are **voluntary measures such as model contract terms** and industry should be consulted extensively during their drafting. As regards the unfairness test, DOT Europe believes that it **should be for the complainant to prove that the terms were unilaterally imposed** as they are best placed to demonstrate attempts to negotiate.

B2G data access rights

The conditions for access by public bodies are not restricted to emergencies but also to much less-defined cases, such as not being able to obtain the data elsewhere. However, Art 15(c) fails to specify a burden of proof for public bodies to provide information which would prove that they used all possible measures in their power to obtain data from the market before using the rights under the 'exceptional need' to request the same data from data holder. This might open the door to misuse, with potentially adverse implications for privacy, IP and trade secret protection We would also support the EC internal scrutiny board's view that a more clear-cut distinction is needed between 'public emergency' and 'exceptional need'. In addition, the data access right is currently too broad insofar as it would cover a situation where the public body could direct the request against a company that merely stores the data on behalf of a third party instead of directing it against that party directly. This would seriously undermine trust in cloud services.

Recommendations

DOT Europe would recommend adopting **tighter definitions of 'public emergency' and 'exceptional need'** and **removing the requirement that data made available to respond to a public emergency pursuant to Art 15(a) be provided free of charge**. It should be clarified that the relevant data holder in this context is the cloud customer, as opposed to the cloud services provider.

Cloud switching

DOT Europe supports the Commission's ambition to make portability and switching easier, but some of the provisions are difficult to implement and risk adversely impacting innovation in the cloud sector.

The prescriptive contractual requirements in Articles 23 and 25 seem to go beyond what is reasonable in a B2B context. For example, a 30-day deadline (extendable to max 6 months) for switching may not be sufficient for moving large amounts of workloads sitting across multiple hosting servers. The requirements to remove all "obstacles" also seems difficult to implement without a specific definition of what may count as one. There might be obstacles that are technical in nature and cannot be circumvented, or that are owed to the new service provider.

A distinction needs to be made between infrastructure-level services (e.g. IAAS for cloud services), which are relatively standardised and commoditised, and software services which are higher up in the application stack (like PaaS or SaaS), which are more complex, often tailor-made, and which are not always perfectly interchangeable from one data processing provider to another. While the proposal recognises such a distinction, the difference in expectations becomes less clear with "functional equivalence" requirements referenced in interoperability provisions. It is not clear what is meant by this and which provider carries the responsibility to ensure it. It is important that services can continue to differentiate their offers and that functional equivalence does not lead or is inappropriately used towards de facto standardisation of services. Mandatory technical specifications for such portability may undermine the aim of creating innovation within the EEA and result in a reduction in consumer choice.

The definition of "data processing services" should not be ambiguous and more clearly focus on cloud services. As currently drafted, it risks inadvertently bring other services in scope creating uncertainty over the scope of the proposed rules for cloud switching and data transfers.

Recommendations

Functional equivalence should be defined more precisely and narrowly. A possible suggestion could be to replace the word 'same' with 'comparable' so that the definition does not impose sameness of service offers and features.

We would also welcome additional clarity on the broad notion of "obstacle" referred to in Article 23 (2) to clarify factors that should be removed during the switching process. Otherwise, it could appear that "technical, organisational or commercial factor" is left entirely to the discretion of a user, creating an impossible compliance obligation.

In addition, given that the cost of processing and porting depends on the complexity, format and size of the data, making egress free of charge would not be appropriate. We would propose **a transparent pricing structure** instead.

International data transfers

Article 27 places additional restrictions on the ability to transfer non-personal data outside the EU, including in response to a third-country government demand, where such a transfer (or access by third-country authorities) may give rise to a conflict with EU or Member State law. For various reasons,

including the broad notion of "conflict" set out in Recital 77, these provisions could create impediments to companies' ability to transfer non-personal data similar to those that the GDPR imposes on personal data. Even if the article is not meant to restrict data transfers, in practice it may become an obstacle to using global cloud services. The lack of clarity on its application is such that it might discourage customers from using a global service if they are worried about their own compliance with the Data Act.

Given extensive legislation in this area we would question the need for further rules and are concerned by provisions which may lead to data localisation. In general, we believe developing international rules is the only way to address this matter. In addition, non-personal data is far less likely to be subject to access requests and does not raise the same kind of risks as personal data. Policy measures should be proportionate to that lower level of risk. Finally, it also risks creating a parallel framework to the ongoing work around Privacy Shield and the CLOUD Act agreement - thereby reducing the positive impact of resolving those issues.

Recommendations

The scope of Art. 27(2) and (3) should be further clarified, in particular as regards what constitutes a conflict with Union law and which steps would be required from a provider in that regard. Since these paragraphs address targeted disclosures, it would be disproportionate to consider that all data transfers under Art. 27(1) should be halted. Finally, the definition of "data processing services" could have implications for transfers going beyond cloud service providers. The current definition is overly broad and ambiguous and should not be drafted in catch-all manner for the sake of future proofing the Data Act.