The EU Data Act – A Good Idea That Needs More Work

In February 2022, the European Commission released its draft Data Act. The proposal is the final prong of the "European Data Strategy" that aims to create a "single market for data," the goal of which is for Europe to attain a commanding role in the global data economy. A report by DigitalEurope, for example, found that under the right circumstances, the EU could create 2 million new jobs and generate about €2 trillion in growth at the end of the decade. Just as important, the Data Act also seeks to remove existing barriers to accessing data and to provide users with greater control over their own data.

As the premier trade association for the information industry, SIIA supports the overall objective of the Data Act to unlock the value of data and foster innovation. In its current form, however, we believe that it would lead to unintended consequences and, therefore, would be likely to do more harm than good—both to European interests and the broader digital economy. Our multi-pronged engagements with both EU institutions and decision makers, and the U.S. government, are aimed at suggesting clarifications and improvements that will allow the Data Act to meet its stated objectives to the benefit of all.

To that end, our concerns with the current version of the Data Act fall, in no order, within four broad categories: restrictions on international data transfers; rules about the sharing of data between businesses and between businesses and governmental entities; the "gatekeeper" exclusion; switching between cloud service providers; and protections for intellectual property and trade secrets.

<u>Restrictions on International Data Transfers</u>

The overarching principle of the Data Act should be to enable and encourage the free flow of data across borders, and rules mandating data localization should be avoided. Anything short of that would be at odds with the goal of maintaining a free and open internet, and it also would not sit well with the newly agreed EU-U.S. Transatlantic Data Privacy Framework, risking confusion over which set of rules to apply and when.

Whether Article 27 of the Data Act is intended to restrict data transfers between the EU and the U.S., its meaning, as written, is sufficiently unclear that, as a practical matter, it might have that effect. Because of this, it is likely to appreciably affect the scope and quality of services that non-EU companies will be able to offer to consumers and businesses within the European Union. We have, therefore, encouraged the EU's institutions to clarify the language of Article 27 to remove any doubt about its actual meaning.

<u>B2B Data Sharing</u>

The Data Act imposes a far-reaching obligation to share data. Article 2(1) defines "data" as "any digital representation of acts, facts or information and any compilation of such acts, facts or information." The definition of the term "related service" is similarly broad. And it sets the conditions under which data must be accessible and can be used. As part of this process, it introduces a "fairness test," under which data must be made available "under fair, reasonable and non-discriminatory terms and in a transparent manner." In Article 13, the draft Data Act defines "[a] contractual term [as] unfair if it … grossly deviates from good commercial practice [and is] contrary to good faith and fair dealing." Article 34 obligates the Commission to develop

model contractual terms in order “to assist parties in drafting and negotiating contracts with balanced contractual rights and obligations.”

SIIA member companies have substantial experience in B2B markets. Their bread and butter is collecting and providing data to other businesses, which is done pursuant to contract. Usually, these contracts are negotiated to achieve specific objectives, including the proper use of the data, protection of intellectual property rights, and remedies for breach, which is both standard and good commercial practice. The above-cited language, however, creates doubt about whether the Data Act seeks to impinge on the fundamental ability of private enterprises to contract freely with each other. Against this backdrop, we believe it would be helpful for the Data Act to state clearly that the principle of contractual freedom, absent exceptional and highly unusual circumstances, should be the norm for B2B data sharing.

B2G Data Sharing

High-quality data is essential for policymaking and for governments more broadly to discharge their duties; many laws and regulations in the EU and its member states already govern the exchange of data between private businesses and governmental entities. Overwhelmingly, this data is shared on a voluntary basis, and we believe that a flexible and voluntary framework that supports B2G data sharing should remain the norm.

Likely based on recent experiences related to the COVID-19 pandemic, the draft Data Act seeks to impose an obligation for private businesses to make data available to governmental entities on an “exceptional need” basis. In Article 15(a), the proposal envisions two scenarios where such a need would exist: first, where the requested data is necessary to respond to a public emergency; and second, where a lack of data makes it impossible for a local authority to perform duties, authorized by law, that are deemed to be in the public interest.

In the abstract, few would deny that a situation could arise that could make it appropriate for a public authority to demand that one or more private businesses turn over data in their possession promptly and free of charge. But the definitions provided in the proposal, of what might constitute “exceptional need,” are unclear and provide a substantial margin of discretion for government officials. This creates not only rule of law concerns for companies, but also raises legitimate questions about whether the Data Act might violate the rights of individuals enshrined in the EU Charter of Fundamental Rights.

Because of this, we recommend that the draft Data Act be amended to provide a clear and very narrow definition of what the term “exceptional need” is intended to mean. In addition, we suggest that the co-legislators provide additional safeguards to protect personal and commercial information, outline the steps that governmental agencies need to take to procure the requested data, and clarify how these new obligations fit within the existing framework of rules and regulations, both at EU and member state level, about B2G data sharing.

“Gatekeeper” Exclusion

One of the primary goals of the Data Act is to empower consumers to take control of their own data and to create more opportunities for them to share that data as they see fit. At the same time, however, the proposal also contains an explicit prohibition against the transfer of any such data to a company that has been designated as a “gatekeeper” under the Digital Markets Act (DMA), which just entered into force. And this carveout applies to all parts of gatekeeper companies, including entities that do not, by themselves, fall within the remit of the DMA.

To begin with, the “gatekeeper” exclusion is completely at odds with what the Data Act claims as one of its most important objectives—to lower, or eliminate, existing barriers that prevent users from sharing their data with whomever they want to share it. The Data Act, as written, also prevents consumers from taking advantage of competitive quality, privacy, security, and performance standards, thereby *limiting* the choice of European consumers, and it discriminates against a select group of, mostly U.S., companies and stops them from competing in this space solely because of their size. For these reasons, we believe that Article 5(2) should be deleted from the proposal.

Switching Between Cloud Service Providers

In Articles 23-26, the Data Act proposal contains a number of provisions related to switching between data processing (cloud) services. There is no doubt that this is an important part of any framework that aims to encourage better access to and sharing of data. Some of the proposed rules raise concerns, however, because they set arbitrary and, as a practical matter, unrealistic timelines.

Article 24, for example, in addition to laying out in fairly granular detail what contractual terms *must* be included in agreements between cloud service providers and their customers, mandates a maximum transition period of 30 days within which such a switch must be effectuated. While time, once a decision to switch has been made, can be a relevant factor, a 30-day maximum deadline would deviate from normal industry standards. In fact, few experts think that a deadline that tight is even practically feasible.

Imposing deadlines that cannot be met serves no one, least of all the companies that will be forced to choose between compliance and doing what is in the best interests of their customers. As a result, we recommend that the co-legislators amend Article 24 to provide a more flexible timeline for the switch between service providers. As a guideline, a minimum timeline of 12 months would put the proposal better in line with current industry standards.

Protections for Intellectual Property and Trade Secrets

In a memorandum accompanying the text of the Data Act proposal, the European Commission itself noted the importance that the protection of confidential business information and trade secrets has for the proper functioning of the EU’s internal market. Simply put: without robust safeguards of these rights, the incentive for businesses to allocate resources to innovation is likely to be negatively affected.

Under Articles 4(3) and 5(8), trade secrets must be disclosed to users and third parties so long as “all specific necessary measures are taken to preserve the confidentiality of trade secrets.” It is, however, unclear what this language would mean in practice, which suggests that no business would have any certainty that its trade secrets will be protected. That is surely not the intent behind the Data Act. We have therefore strongly encouraged the co-legislators to amend these provisions to clearly spell out that there is no obligation to share, with users and third parties, trade secrets within the meaning of the Trade Secrets Directive. As the special law (*lex specialis*) governing this specific issue, the protections enshrined in the Trade Secrets Directive should take precedence.

We also have serious concerns about the Data Act’s treatment of intellectual property rights. The forced transfer of source code, for example, would create both policy and legal risks. Not only is it likely to put a damper on innovation, it will also discourage cross-border data sharing—

one of the main goals behind the Data Act—for fear of disclosure. Because of this, we believe that Article 35 should be clarified to make it clear that it does not expand or diminish existing copyright protections in any way.

The EU Commission has an ambitious agenda, which focuses on regulating a broad swath of the digital economy. This approach enjoys broad support among citizens and elected officials in Europe, and it has certainly put the EU on the map as a regulatory superpower. But it is not cost-free. None of the dominant tech platforms emanate from the Old Continent, and every new piece of legislation adds additional complexity to an already sprawling and complicated rulebook. Because of this, Europe runs the risk of creating a regulatory framework that will deter, rather than spur, necessary investments in innovation, thereby leaving companies and consumers, in Europe and beyond, worse off. We believe the above recommendations will significantly improve the draft Data Act and provide greater consistency with other elements of the EU's digital agenda.