U.S. Chamber of Commerce

The EU Data Act: A Misguided Policy

Forced Data Sharing & Restricted Data Flows Would Harm Economy, Undermine Cooperation

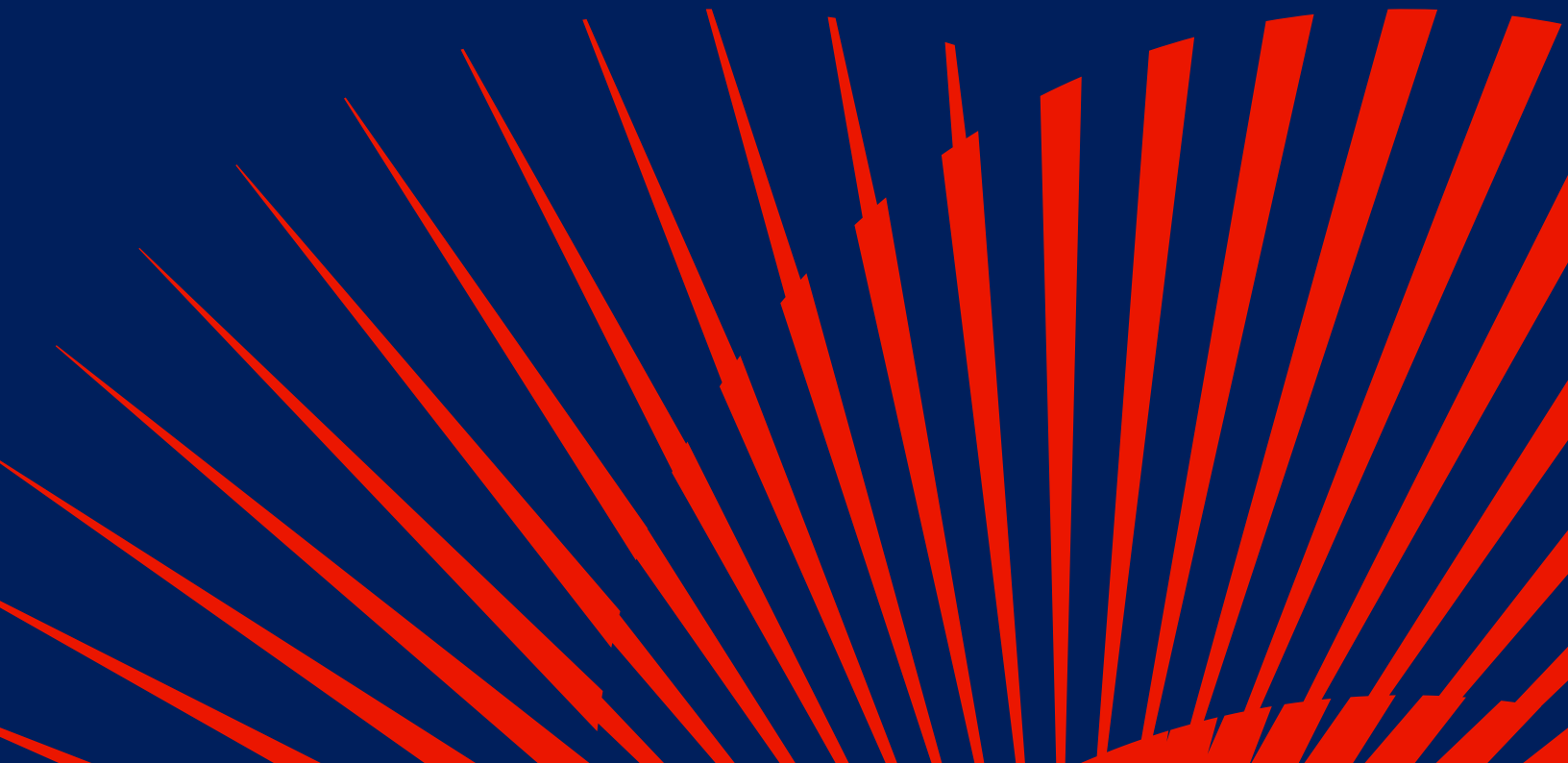


Table of Contents

The Chamber thanks WilmerHale LLP for its assistance in preparing this report.

Introduction

On February 23, 2022, the European Commission introduced a proposal for a "Regulation on harmonized rules on fair access to and use of data," which it labeled the "Data Act."[1] The Data Act will introduce a complex and burdensome regulatory scheme governing the use of personal and non-personal data in Europe, should it become law. In addition to violating international trade rules, this scheme will negatively impact companies in nearly every sector of the economy that do business in Europe—notably including major U.S. investors in Europe.

Any U.S. company that manufactures products sold in Europe that generate data, provides services in Europe allowing such products to perform their functions, provides data processing services (*e.g.*, cloud services) in Europe, or is otherwise considered a "data holder" in Europe, could experience direct economic harm, as will many users of their products and services. The U.S. economy and U.S. workers would suffer as a result, given that the EU is the United States' largest export market and the leading destination for foreign direct investment.[2]

The purpose of this white paper is to alert policymakers to the potential consequences of the Data Act, especially if implemented in its current form, and to urge them to take all appropriate steps to discourage the EU from bringing the measure into law. Despite its name, failure to act now would have consequences far beyond the digital economy or technology sector.

Autos: The EU is one of the United States' leading export markets for automobiles and the Data Act's provisions compelling data transfer when connected products generate data will have a significant impact on the global automotive industry.

Aviation: The Data Act risks undoing a highly functional data-sharing regime that is already serving the interests of both data holders and users. If the Data Act imposes requirements on manufacturers that undermine their ability to protect trade secrets and other intellectual property, the logical response will be to reduce the amount of data they collect. The result will be less innovation and higher costs, leaving the entire sector worse off than it is today.

Digital Services: The EU designed the "gatekeeper" concept to impose discriminatory rules on a handful of specific U.S. technology companies to limit their ability to compete in the EU. The Data Act will also force gatekeepers to incur significant costs to modify their products and related services and face legal/compliance risk, while they are excluded from the benefits of data sharing that the Data Act purports to create.

Pharmaceuticals and medical devices: Trade secrets and other intellectual property rights are the cornerstones of the pharmaceutical industry and key driving forces of innovation. Patented methodologies, clinical data, and other proprietary information reflect years of research and investment by pharmaceutical companies. Therefore, the pharmaceutical industry is particularly vulnerable to the disclosure of trade secrets and other intellectual property under the data sharing requirements of the Act. Meanwhile, restrictions on cross-border data flows for industrial data will undermine clinical trials and impede necessary regulatory data exchange.

Financial services: Data sharing is an industry norm and financial institutions regularly enter into complex data sharing agreements. In the business-to-business context, these complex agreements will be disrupted by requirements under the Data Act limiting contractual freedom, which will also restrict the ability of financial institutions to negotiate new contractual arrangements to address novel issues such as FinTech.

The Data Act is not an isolated measure. Rather, it is the latest manifestation of the EU's "technological sovereignty" agenda, which seeks to elevate European companies at the expense of non-European companies using regulatory policy. The Data Act follows the Data Governance Act, the Digital Services Act, the Digital Markets Act, the draft Artificial Intelligence Act, along with other measures including the forthcoming Carbon Border Adjustment Mechanism in this regard.

Our specific recommendations are as follows:

U.S. policymakers should signal clearly to the European Commission that the Data Act as currently constituted is unacceptable. The Commission is currently considering revisions to the measure to address some concerns that have been raised by stakeholders.[3]

U.S. policymakers should urgently engage their European counterparts to develop an alternative approach to the regulation of data in the global digital economy that prioritizes contractual freedom between economic operators, voluntary data sharing, and non-discrimination. The U.S.-EU Trade and Technology Council, if properly leveraged, could be one suitable venue for such discussions.

EU policymakers should halt further consideration of the Data Act pending discussions with the United States and other likeminded countries regarding legitimate concerns with the measure. It would be a major loss for transatlantic economic cooperation if the Data Act were to become law while serious issues between the United States and the EU with respect to the measure remain unresolved.

U.S. policymakers should prepare, if necessary, to use domestic or international enforcement tools–including but not limited to WTO dispute settlement–to discourage the EU from following through on the Data Act. Other recent disputes could have been mitigated had the United States engaged European counterparts more proactively or considered such tools. It is critical that the United States not wait this time, given the massive impact that the Data Act would have on U.S. companies and European firms with significant investments across the United States.

International policymakers should not emulate the Data Act. Forcing companies that invest in your country and provide goods and services to your citizens to transfer critical data and sensitive information to their competitors will impede future investment. It will also undermine innovation: companies will think twice before committing the resources necessary to innovate if their success will be met with targeted, discriminatory regulation, especially ones designed primarily to benefit local "national champions."

The paper is divided into three parts.

Section I summarizes the key features of the Data Act, including its purpose and scope and main provisions, with the understanding that several aspects of the Act are still under review by the European Commission, European Parliament, and the 27 EU member state governments.

Section II explains the impact of the Data Act on U.S. companies that conduct business in Europe. Sub-section A sets out the challenges. Sub-section B looks at how these challenges will impact specific sectors, as described above.

Section III explains how the Data Act is inconsistent with the EU's international trade obligations. It raises serious concerns under the rules of the World Trade Organization, implicating several agreements, including GATT 1994, the TRIPS Agreement, the TBT Agreement, and GATS.

I. Overview of The Data Act

A. Purpose and Scope

According to the European Commission, the primary objective of the Data Act is to better utilize industrial data generated in the EU single market for the benefit of Europeans, as such data—it is asserted—is mostly "unused" or "its value is concentrated in the hands of a relatively few large companies."[4] The Data Act seeks to achieve this goal by (1) introducing user rights to access data, both personal and non-personal, generated by products or related services; (2) requiring transfers of this data to third parties to be made under fair, reasonable, and non-discriminatory terms, while at the same time precluding companies deemed "gatekeepers" under the Digital Markets Act from receiving this data; (3) mandating business-to-government transfer of data in certain circumstances; and (4) regulating data processing service providers, including rules to facilitate switching between data processing services and imposing new restrictions on international transfers of industrial data.

B. Main Provisions

1. Users have the right to access data generated by products and related services

Manufacturers of products and providers of related services that generate data are governed under the Data Act as "data holders."

The Data Act imposes an obligation on data holders to provide users access to personal and non-personal data generated by using the product or related service. Upon request from a user, which may be an individual, or a legal entity, as well as the owner, borrower or lessee of the product in question, the data holder must provide the data "without undue delay, free of charge and, where applicable, continuously and in real-time."[5]

Data holders are required to provide users with certain information before entering a contract for the purchase, rent, or lease of a product or related service, including the nature and volume of the data to be generated by the use of the product or service, how the user may access the data, and how the user may request that data be shared with a third party.[6] Data holders may not use data generated by products or related services beyond the scope of the contract with the user.[7] As for the user, where it requests access to data generated from its use of a product, the user may not use such data to develop a competing product.[8] While the development of "a new and innovative product or related service" remains possible,[9] it is a distinction that will not be easy to make in practice, because the definition of the relevant market remains unclear, despite being the core condition for such assessment. The draft Data Act also does not discuss safeguards for forced data transfers to companies offering competing products which already exist.

The Data Act also requires that "[p]roducts shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user."[10]

2. Users have the right to require data to be transferred to third parties, excluding gatekeepers

In addition to making data accessible to the user, data holders must also make the data available to third parties if the user requests, "where applicable, continuously and in real-time."[11] Third parties are known as "data recipients" under the Data Act and include persons, businesses, research organizations, or not-for-profit organizations.[12] However, the Data Act specifically prohibits the transfer of personal and non-personal data to companies designated as "gatekeepers" under the existing Digital Markets Act.

The Data Act requires the data holder to make the data available to a data recipient under "fair, reasonable and non-discriminatory" ("FRAND") terms–including payment of "reasonable" compensation–and in a transparent manner.[13] The data holder may utilize smart contracts to prevent unauthorized access to the data.[14] Disagreements regarding terms may be resolved through dispute settlement bodies established by individual Member States.[15]

The Data Act imposes certain limitations on the data recipient's use of the data. For example, the data recipient may not use the data for "profiling" natural persons or transfer the data to a third party (unless necessary to provide the service requested by the user), transfer the data to a gatekeeper; or use the data to develop a competing product.[16]

3. EU governmental entities can access data where there is an exceptional need

Data holders must make data available, without undue delay, to a public sector body or an EU institution or agency when such an entity demonstrates an "exceptional need."[17] The Data Act provides a list of circumstances when an exceptional need will be found to exist, including where the data is necessary to respond to a public emergency, and where the lack of available data prevents the entity "from fulfilling a specific task in the public interest that has been explicitly provided by law" and the entity has been unable to obtain the data by alternative means.[18] The Data Act allows a data holder to decline or seek a modification to a governmental request for data under certain conditions, which the governmental entity may challenge before a designated competent authority.[19]

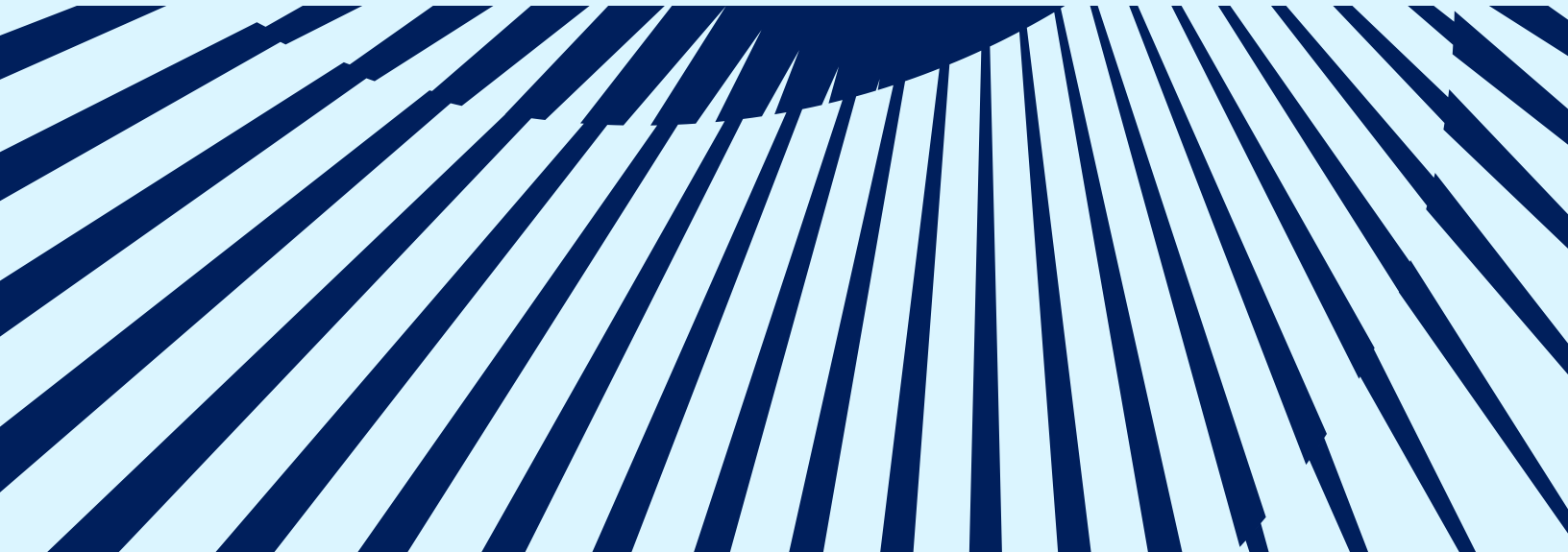
4. Data processing service providers are subject to new rules regarding switching, international data transfer

In addition to the provisions for data holders and data recipients, the Data Act also establishes new requirements for providers of data processing services.[20]

The Data Act requires that data processing service providers take various steps to ensure that their customers can switch to another data processing service. Providers are required to support their customers to ensure that the switching process is effective and successful.

Such support includes removing any commercial and contractual barriers that prevent a customer from: terminating a service contract; concluding new contracts with one or multiple data processing service providers covering the same service type; and porting data and other digital assets to other service providers.[21] Further, providers of certain types of cloud services are subject to additional technical requirements to facilitate switching. Providers of cloud infrastructure services (*i.e.*, infrastructure-as-a-service, or IaaS), must ensure that their customers "enjoy[] functional equivalence in the use of the new service" after switching.[22] Providers of cloud application services (*i.e.*, software-as-a-service, or SaaS) and cloud platform services (*i.e.*, platform-as-a-service, or PaaA) must ensure compatibility with open interoperability specifications or European standards for interoperability.[23] These specifications and standards must ensure functional equivalence "where technically feasible."[24]

The Data Act also restricts international data sharing by data processing service providers. Providers must take "all reasonable steps" to prevent international transfer or foreign governmental access to non-personal data held in the EU where such transfer or access would conflict with the law of the EU or its member states.[25] The Act also bars the enforcement of any order from a foreign country's courts or administrative authorities requiring the transfer of non-personal data unless the request is based on an international agreement or the third country's legal system affords certain enumerated protections.[26] If the conditions are met, data processing service providers are required to inform the data holder about the third-country request before complying with the request, subject to certain exceptions.[27]



II. The Data Act Would Hurt Companies Across Numerous Sectors

In complementing existing EU law, like GDPR, and the Data Governance Act, the EU Data Act can play a crucial role in unlocking the use and re-use of industrial data in the EU where there are no existing frameworks. Proportionate access, sharing, and use of data is central to innovation and should be facilitated through clear regulatory intervention and guidance. It can power the digital transformation of businesses and organizations of all sizes, through artificial intelligence and other data driven innovations, and support governments and researchers in tackling the most fundamental challenges of our time, from climate change to fighting the COVID-19 pandemic. For this reason, we support the European Union's principle of bolstering sharing of industrial data across territorial and organizational boundaries, and its willingness to create a frictionless single market for data.

Many of the companies which the U.S. Chamber represents have been at the forefront of advocating for such frameworks to unlock the potential for data sharing across the economy. In developing and participating in leading data sharing projects, such as the Data Transfer Project, their experience with data sharing has provided valuable insight.

However, in aligning with existing EU frameworks, a careful balance must be struck between bolstering data sharing, preserving the privacy and safety of users, securing the integrity of products and services, and incentivizing innovation by securing and enforcing strong protections for intellectual property rights and trade secrets.

In contemplating a new regime with requirements and obligations on the transfer of non-personal data to third countries, there is a significant risk that such transfers may face similar or even more significant barriers than seen regarding the transfer of personal data from the EU to the United States over the past several years.

It is essential for the transatlantic digital economy, and the global digital economy more broadly, that such transfers—for both personal and non-personal data—are robustly protected and organizations have legal certainty regarding their obligations.

As currently considered, the Data Act would have far-reaching, often negative, effects on companies that operate in Europe in numerous sectors, no matter their nationality. Any company from any jurisdiction that, for example, manufactures products sold in Europe that generate data from their use, would face new limits on its ability to compete and innovate based on their use of such data, as well as significant legal and regulatory risks. All the while, the Data Act is unlikely to succeed in accomplishing its goals of helping European companies make better use of data or growing the EU economy.

A. Key Challenges for Companies

Companies that conduct business in Europe, including and especially U.S. companies, will encounter the following key challenges if the Data Act becomes law without significant amendments:

1. The Data Act will penalize competition on the merits and chill investment and innovation

The Data Act is a significant threat to the procompetitive business models of companies that generate or process data in Europe. Through their ingenuity, risk-taking, and expenditure of capital and other resources, these companies have created products and services that have unlocked the benefits of data for consumers and businesses in Europe and around the world. By means of the Data Act, the European Commission's proposed response is to punish these companies–not because they have amassed market power that raises concerns under competition law–but because the Commission speculates that prescriptive regulation will stimulate greater and fairer utilization of data. This is the wrong approach. It will penalize competition on the merits across all sectors of the economy and stymie investment and innovation.

In the case of products and related services, the requirement in the Data Act to transfer data to users and to third parties is akin to the expropriation of property.

Manufacturers and service providers derive significant competitive advantages from access to the data that their products and services generate. They and their clients can already negotiate favorable and mutually agreeable terms for the sharing of that data, without government mandates. Behind the elaborate scheme of data users, data holders, and data recipients, the Data Act reflects a simple proposition: these companies should be compelled to relinquish their hard-earned competitive advantages, without sufficient safeguards for their hard-earned intellectual property.

This is particularly costly in the case of derivative data. Despite ongoing deliberations within the EU, the current draft does not provide sufficient comfort that derivative data that results from software or hardware processes applied to raw data will be excluded from data transfer requirements. Any requirement to disclose derivative data—which is likely to be embedded with trade secrets or other proprietary information—would deter investment from the European market and encourage companies to innovate elsewhere.

Apparently recognizing these risks, the Commission included two provisions in the Data Act to "maintain[] incentives for manufacturers to continue investing in high-quality data generation": (1) "covering their transfer-related costs"; and "excluding use of shared data in direct competition with their product."[28] We are concerned that neither purported safeguard will be effective.

First, with respect to compensation, the product manufacturer or service provider will not receive any compensation for transferring data to users, and compensation may also be unavailable for transferring data to data recipients.[29] Even where the product manufacturer or service provider is entitled to compensation from a data recipient, the right to "reasonable" compensation–on FRAND terms–will likely invite controversy and litigation, as discussed below. The small possibility of compensation, therefore, does not mitigate concerns that the Data Act will stifle investment and innovation.

Second, with respect to competing products, while users and data recipients are prohibited from using data they receive from data holders to develop competiΩng products, they are *not* prohibited from developing competing services or a different category of products.[30]

A data recipient can also pass data to other parties "if necessary to provide the service requested by the user," enlarging the universe of risk.[31] Even if a data recipient uses data it receives improperly, it can continue to do so if the data holder has not suffered "significant harm" and a penalty would be "disproportionate."[32] These various loopholes create a substantial risk that data transferred by a product manufacturer or service provider will be used against it. This threat is likely to further undermine investment and innovation by manufacturers and service providers.

The Data Act will have a similar impact on data processing service providers. It imposes switching obligations on cloud service providers where the associated costs will disproportionately fall on U.S. CSPs because of both their customer base but also maturity and complexity of their service portfolio. Although the Data Act does not expressly require data processing service providers to transfer data to third parties, it is anticompetitive at its core: indeed, it expressly requires service providers to help their customers switch to competing service providers.[33]

The provisions requiring providers of cloud services to ensure "functional equivalence" in the use of the new service to facilitate switching may make it impossible for providers to differentiate themselves in the market based on their distinct services, potentially ushering in a race to the bottom rather than incentivizing innovation and the development new features.[34] The current definition of "functional equivalence" does not leave room to address differences in service quality among cloud service providers. Functional equivalence should not preclude difference in service quality or other differentiating factors among cloud service providers. Instead, a more proportionate approach is warranted, as it is not feasible to ask the outgoing provider to provide "functionally equivalent" services as the incoming providers, if this means forcing providers to essentially build the exact same features.

The focus should instead be on removing on artificial barriers to switching. The Data Act requires CSPs to pay most, if not all, switching costs when their customer leave to another provider, even if CSPs have no visibility or control over these costs.

Without evidence of these costs preventing effective competition in the wider IT industry, such a stringent measure is not economically justified and will lead to negative externalities, such as price increases for customers that do not even intend to switch. This will likely reduce incentives and the ability to invest in innovation, keep prices low and actually reduce the speed of cloud take up as a result. Further, the Data Act does not include any provisions seeking to maintain data processing service providers' incentive to invest and innovate or even continue to provide their services to European customers—not even the flawed safeguards discussed above pertaining to manufacturers of products and providers of related services.

In all, the Data Act imposes obligations on companies that generate or process data in Europe to facilitate data transfer to their competition without sufficient safeguards for IP rights. This is perhaps the greatest threat posed by the Data Act. We are concerned about the future attractiveness of the European market for investment and innovation across a range of product and services sectors if the Act moves forward in its current form.

2. The Data Act will force companies to share trade secrets and other sensitive information with their competitors and EU governmental entities

The Data Act requires data holders–including but not limited to manufacturers of products and providers of related services that generate data–to transfer data to three different actors: (1) to users of the products or related services; (2) to third-party data recipients upon request by a user, *e.g.*, to obtain aftermarket services; and (3) to EU governmental entities. In each of these scenarios, the data that the Data Act requires the data holder to transfer can include or reveal the data holder's sensitive information, including trade secrets, other intellectual property, and business confidential information. This poses an unacceptable risk of harm to the data holder.

Take the example of trade secrets. For many companies, trade secrets are the company's most valuable assets. They are the "secret sauce" that enable a company to distinguish its goods and services from its competitors' goods and services, win and sustain market share, and deliver value to its customers.

They represent significant investment by companies–including companies that manufacture products and provide related services that generate data–to drive innovation and competition. But a trade secret will lose a substantial portion of its value if it is no longer secret and if other actors, including competitors, can utilize and profit from it. That is why companies expend enormous resources to safeguard their trade secrets.

Against this backdrop, the Data Act *expressly requires* data holders in certain circumstances to transfer trade secrets to users of their products and related services; to third parties, which may be their competitors; and to EU governmental entities which have no fiduciary responsibility to protect this information. The protections for trade secrets required by the Data Act are weak and ineffective.

Data holders must transfer trade secrets to users of their products and related services where "all specific necessary measures" are taken by the user to protect the confidentiality of the trade secrets.[35] While the proposal states that the data holder "can" agree on terms to protect the data, it does not mandate that such an agreement be made, nor provide guidance regarding the measures a user must take to ensure the protection of the trade secret.[36] There is also reason to question whether any confidentiality agreement can adequately safeguard trade secrets. Data holders must also transfer trade secrets to third-party data recipients, if requested by the user, if such disclosure is "strictly necessary to fulfil the purpose agreed between the user and the third party" and all "specific necessary measures agreed between the data holder and the third party are taken by the third party to preserve the confidentiality of the trade secret."[37] Again, however, the proposal does not appear to require the third party to enter into such an agreement, nor provide a means for the data holder to monitor and enforce compliance. Therefore, more robust safeguards for trade secrets are necessary. For example, the data holder should be able to revoke sharing of data that contains trade secrets if the user or third party does not properly implement the agreed-upon technical measures to preserve confidentiality or if it breaches those measures.

There are also loopholes. For example, such agreements and other protection measures will be invalid if, for example, they are determined to have been "used as a means to hinder the user's right to effectively provide data to third parties"[38] or if they are "unilaterally imposed" on SMEs and contain "unfair" terms.[39] However, the problem with the definition of "unilaterally imposed" is that it sets the threshold too low: it would allow any contractual partner to argue a contractual term is unfair merely because it did not get its way during negotiations. These exceptions may result in the exposure and loss of trade secrets, depending on how they are interpreted. In order to prevent potential misuses of this provision, the focus should be on whether the contractual partner was given an opportunity to negotiate the term in question.

Finally, data holders must transfer trade secrets to EU governmental entities when it is "strictly necessary to achieve the purpose of the government's request"[40] for data to meet an "exceptional need." Problematically, despite inconclusive ongoing EU deliberations on this point, the threshold for exceptional need appears quite low. While preventing public emergency may be a defensible instance of exceptional need, the proposal also allows EU governmental authorities to compel the transfer of data (including trade secrets) in a wide range of other "public interest" circumstances.[41] This means that companies' trade secrets could regularly be transferred to EU governmental authorities which request them. While the government is required to take "appropriate measures" to protect the confidentiality of the trade secrets, it is not required to negotiate or enter into an agreement with the data holder regarding such measures, which appear to be at the governmental entity's sole discretion.[42] Further, unlike companies which have responsibilities to their shareholders to protect their intellectual property and invest heavily in their cybersecurity, this information is likely to be at greater risk to industrial espionage or successful cyberattacks by adversarial nations if held on government servers.

All these mandated transfers endanger trade secrets and the competitiveness of their owners. In the case of data transfers to users—and potentially, data recipients as well—data holders will not receive compensation, adding insult to injury.[43]

The situation in the case of other types of intellectual property and confidential business information is even more stark. While the Data Act includes some, albeit flawed, protections for trade secrets, it provides no tailored protections for other sensitive information, including other types of intellectual property and confidential business information[44]–on the contrary, it expressly lowers certain protections.[45] This creates significant risks for data holders subject to the transfer requirements in the Data Act.

The discussion above focuses on companies that are considered data holders, including product manufacturers and providers of related services. But data holders are not the only ones that the Data Act forces to transfer trade secrets, other types of intellectual property, and business confidential information to their competitors. Providers of certain data processing services across a range of industries and sectors will also be forced to do so, albeit not expressly.

U.S. cloud service providers will find it extremely difficult, if not impossible, to comply with new requirements to provide "functional equivalent" services without being forced to divulge critical trade secrets, other types of intellectual property, and business confidential information with other cloud service providers–their competitors. And there are no provisions in the Data Act requiring the recipients of such information to keep it confidential or refrain from exploiting it for their own commercial purposes.

The damage caused by these rules requiring companies that generate or process data in Europe to share their trade secrets, other types of intellectual property, and business confidential information is not limited to the companies themselves—the economic competitiveness and national security of the United States and our allies may also be at risk. For example, there is nothing in the Data Act that would prevent users to compel data holders to transfer sensitive information to an ostensibly European company that is actually a Chinese state-owned shell company. In this way, the Data Act could enable or other countries of concern to obtain access to sensitive information, such as strategically important technical know-how that they would have been unable to obtain through voluntary contractual arrangements, to the detriment of core U.S. economic and even security interests.

Acquiring data through a Data Act request could be one way for sanctioned entities or state-owned enterprises from adversarial nations to avoid carefully targeted export controls or investment restrictions, for example.

3. The Data Act will drag firms into expensive and uncertain litigation and subject them to massive fines by regulatory authorities

The Data Act will subject companies that are considered data holders to significant litigation risk that will increase their cost of doing business, perhaps substantially. Some of this risk is by design—for example, the Act anticipates extensive litigation over whether a data holder has met its obligation to provide data to a data recipient on FRAND terms (which remain undefined), and it creates new dispute settlement mechanisms to handle such disputes. Other litigation risk results from ambiguities in the proposal regarding key language and concepts, such as "data holders" and "functional equivalence." In addition to litigation risk, companies will be vulnerable to massive fines by EU governmental authorities that have been more than willing to use such coercive measures against firms, especially foreign-headquartered ones, in the recent past.

With respect to litigation risk, the FRAND provisions stand out. The Data Act inappropriately borrows the FRAND concept from the standard essential patent context.[46] In the standard essential patent context, a FRAND commitment is the result of a voluntary agreement to contribute a patent to a standard. Here, the FRAND commitment is not the result of a voluntary agreement, but rather a government mandate. In the standard context, FRAND terms are frequently litigated, and fraught, issues in intellectual property law. By incorporating and mandating a FRAND obligation via government regulation to the terms of data transfers between data holders and data recipients, the Data Act creates a new litigation cottage industry targeted at data holders. Litigation will likely be even more prevalent in this space given that "the informational value of the data and intended uses are unlimited," while standard essential patent licensing primarily focuses on telecommunications standards.[47]

The drafters of the Data Act acknowledge, and attempt to address, this obvious concern by creating new dispute settlement mechanisms to handle the disputes. These new mechanisms are required to be impartial and independent, include expertise in the subject matter, and capable of issuing decisions in an efficient and cost-effective manner.[48]

But even if these dispute settlement mechanisms prove better than domestic courts in resolving FRAND disputes, the disputes would still be costly and time-consuming for data holders. Also, the dispute settlement mechanism may not be available when it counts: it will only be empowered to issue a binding decision if the parties to a dispute consent in advance, which is not guaranteed.[49] Even if a mechanism is available and capable of issuing binding decisions, there may still be further litigation. While a mechanism created under the Act may not hear a dispute that has previously been submitted to a domestic court, it appears that a party that is dissatisfied with a decision by a mechanism can turn to domestic courts for a second bite at the apple.[50] All of this risk harms the commercial position of the data holder.

In addition to the greater frequency of costly disputes, it seems likely that data holders will lose more than they win, adding further risk. That is because data holders are presumed guilty when challenged. Under the Act, if a data recipient alleges that a data holder's proposed data transfer terms do not meet FRAND requirements because they are discriminatory, the data holder bears the burden to disprove the allegation.[51]

In these ways, significant litigation risk for data holders is baked into the Data Act. It is a feature, not a bug, meant to skew incentives and pressure data holders to transfer data to other, perhaps less innately competitive, companies on generous terms. But then there are ample bugs in the proposal as well, including a litany of vague terms and concepts that make compliance with the proposal difficult and frequent litigation seemingly unavoidable. The following are key examples of ambiguities that will have a major commercial impact if the Data Act becomes law:

Raw data v. derivative data. Despite ongoing deliberations within the EU, the Data Act as currently drafted does not adequately distinguish between raw data and derivative data.

Data holders are required to transfer data "generated by the use of a product or related service" to consumers and businesses, but this language is not defined.[52] The preamble clarifies that it excludes "data resulting from any software process that calculates derivative data from such data as such software process may be subject to intellectual property rights."[53] However, this language does not provide sufficient comfort that derivative data will be excluded from data transfer requirements. Companies that withhold derivative data risk litigation, and those that disclose face a heightened risk of losing trade secrets and other proprietary information.

Personal v. non-personal data. The Data Act applies to both personal and non-personal data. Practice in recent years has demonstrated that it can be far from clear in many situations which data are personal data, and which are not. In addition, with respect to personal data, the text confirms that the Data Act "shall not affect" the applicability of the GDPR or other EU law regarding the protection of privacy. But that only begs the question: how, for example, can a data holder transfer data to a data recipient "continuously and in real-time," as required by the Data Act, while also distinguishing personal data from non-personal data and meeting its requirements under EU data protection and privacy laws with respect to personal data? Data that is encrypted, aggregated, anonymized, or stored on-device and therefore not accessible to the data holder, should not be shared. The challenges compound when the personal data of multiple people is intermingled, such as when multiple family members or colleagues use a given product. Failing to address these complexities and legal inconsistencies puts data holders in an impossible situation. The litigation risk is considerable.

Data holders. Where multiple companies may be jointly involved in manufacturing connected products and providing related services, it will often be difficult to identify the data holder, *i.e.*, the company that has "the ability" to make available certain data. Litigation can be expected to fill the gap. This is unfortunate and unnecessary, as the sales contract between a user and a product manufacturer or service provider is better situated to identify the data holder. Outside this environment, there are other issues with data holders. The definition of the term extends to any person with "the right or obligation" under "applicable Union law or national legislation implementing Union law" to make available certain data.[54]

As such, there are whole categories of persons outside of companies that manufacture products or related services that generate data that may be required to make available data to consumers or businesses on FRAND terms, for example. Absent clarification, litigation will ensue, and the courts will decide on the basis of the ambiguous language in the proposal.

These ambiguities in the Data Act do not just subject data holders, including U.S. companies, to litigation risk; massive fines by EU governmental authorities are also on the horizon. Under the Data Act, the EU data protection authorities may impose fines of up to €20 million or up to 4 percent of total worldwide turnover in the preceding financial year for breaches of the rules pertaining to transfers of data to users of products or related services, third-party data recipients, and EU governmental entities.[55] Further, for breach of the rules pertaining to transfers of data to EU governmental entities, the European Data Protection Supervisor may impose an additional fine of €50,000 per infringement and up to €500,000 per year for breach of the rules.[56]

These types of significant fines will undermine the European investment climate—especially considering how EU data protection authorities have shown their willingness to use them to address breaches of other data rules. While GDPR-related fines on technology companies may draw the most attention, EU data protection authorities have imposed such fines on companies in numerous sectors.[57]

4. The Data Act will impair companies' access to state-of-the-art cloud services, artificial intelligence, and other advanced technology

The Data Act's rules related to data processing services and the connected products and related services will impair companies' access in the EU market to advanced technology, including cutting-edge cloud services and artificial intelligence. This will negatively impact companies' ability to innovate in Europe and elsewhere and develop goods and services to meet society's needs.

Beginning with data processing services, the Data Act sets out requirements for a subset of data processing services–cloud services–that will reduce the quality and variety of such services that are available in the EU market, with cascading impacts in other markets.

In particular, the Data Act (a) requires incumbent cloud infrastructure service providers to ensure that their customers "enjoy[] functional equivalence in the use of the new service" after switching;[58] and (b) requires incumbent cloud application service providers and cloud platform service providers to employ open interoperability specifications or European standards that ensure functional equivalence "where technically feasible."[59] It is unclear how an incumbent can guarantee the level of service offered by another service provider in a technical environment under which it has no control. But even assuming functional equivalence were achievable, the results would be devastating for customers of cloud infrastructure services, including U.S. companies.

To ensure functional equivalence, cloud service providers would be forced to align their services, rather than compete based on their distinct offerings. The resulting homogenization of cloud infrastructure services would stunt, or even reverse, the current market trend of rapidly expanding types of cloud services available to customers. It would also undermine innovation in sectors that depend on advanced cloud services capabilities.

The Data Act includes additional requirements ostensibly meant to help customers switch to new cloud service providers that will be unachievable in some cases–subjecting U.S. cloud services companies to large fines that would undermine their market position–and in other cases, result in a flawed or incomplete switching process for customers. For example, the Data Act imposes a fixed term notice period of 30 days for customers to terminate the contract. This will prevent the practice of cloud customers and providers from agreeing on any financial or negotiated commitments in a fixed term agreement, allowing for financial forecasting and planning of activities that benefit both parties. Moreover, the Data Act requires switching to occur within 30 calendar days.[60] This timeframe is infeasible for certain service providers, such as providers of cloud application services.[61] For other service providers, 30 days may be achievable, but risky. The switching process is a costly, complex, and fragile project that requires cooperation between the incumbent service provider, the new service provider, the customer and, at times, outside technical advisors. Imposing arbitrary time limits increases the risk of data loss and other negative business impacts for customers during the switching process.

In addition, without any economic justification, data processing service providers will no longer be allowed to charge for costs associated with the switching process when a customer decides to leave. As costs need to be recouped somehow, this would affect all customers, switching and non-switching, creating negative externalities including increased costs across the board.

In sum, the consequences of the ill-conceived functional equivalence requirement and other switching requirements, including arbitrary time limits, will hurt U.S. companies that depend on the cloud. Further, they will hurt U.S. cloud service providers themselves, which are the world's leaders in the sector.[62]

As for connected products and related services, the Data Act's rules in this space will also limit the availability and development of advanced technology to the detriment of U.S. companies. Two examples are noteworthy.

First, the Data Act provisions that exclude gatekeepers (designated under the Digital Markets Act) from data access rights will block consumers and businesses from benefiting from services provided by the world's leading technology companies. If a company manufactures products or provides related services that generate data, or provides data processing services, it will be required under the Data Act to transfer sensitive information, including trade secrets, to its competitors.[63] However, a gatekeeper may not access data generated by other such products or related services under the Data Act, *even where a user of such products or services wishes to grant a gatekeeper such access*. Today, users turn to companies that will likely be designated as gatekeepers for a range of services in relation to their data, including data analytics, artificial intelligence, and machine learning services. If the main objective of this proposal is to increase user choice and competitiveness, excluding certain companies from the outset limits the potential consumer benefit and reduces the incentive for those companies to build tools to facilitate portability. If the Data Act becomes law, users will be prohibited from contracting with gatekeepers for such services in relation to data they obtain under the measure.

Gatekeepers are not the only companies that will suffer as a result. Any company, including U.S. companies, that wants access to cutting-edge services in the EU market that may be provided exclusively or most efficiently by gatekeepers will be denied such access. This technological embargo will frustrate companies' efforts to use data–including data generated by their own use of products or related services and data transferred by other users of such products and services–to develop new commercial offerings. Moreover, contrary to the intentions of European policymakers, many of the perceived benefits of denying gatekeepers access to this data will instead flow to state-owned enterprises from China and other adversarial countries.

Second, the Data Act provision prohibiting data recipients from using data they obtain under the measure for "profiling" persons, unless it is necessary to provide the service requested, will also curb the development of advanced technology applications valued by U.S. companies–in particular, artificial intelligence. Profiling is the use of personal data to analyze or predict behavior or other attributes of individuals.[64] It is an essential tool in training algorithms used in artificial intelligence. Barring companies from profiling—which, importantly, deviates from the approach taken under GDPR—will frustrate the development of this important technology in the European market. Additionally, these requirements appear inconsistent with the nominally risk-based approached envisioned under the forthcoming EU AI Act.

5. The Data Act will threaten companies' ability to transfer data out of Europe

By means of the GDPR, the EU created a system of restrictions on the transfer of personal data outside Europe. The Data Act goes a step further: it restricts the international transfer of *non-personal* data by providers of data processing services, and on vague and uncertain grounds. This radical new approach to non-personal data, which inherently maintains no right to privacy, threatens to prevent U.S. cloud service companies from transferring data to the United States whether on their own accord or at the behest of their customers for optimal processing, storage, and other use.

It will thereby significantly raise the costs of doing business for U.S. companies and create new risks as well, including cybersecurity and privacy risks, for data that must be processed and stored in Europe. Strangely, data transfer requirements will actually be more stringent for non-personal data than for personal data once the new EU-U.S. Data Privacy Framework is fully implemented.

The Data Act requires providers of data processing services to take all reasonable steps to prevent the international transfer of non-personal data held in the EU where such transfer would conflict with the law of the EU or its member states.[65] This broad language appears to openly invite EU and member state policymakers to develop restrictions on cross-border flows of non-personal data. Further, it will be difficult for any company, but particularly a small or medium-sized company, or a data processing services provider (which in most cases do not access client data), to determine with certainty whether an international transfer conflicts with EU or member state measures, or if the company has taken "all reasonable steps" to prevent such transfers. As such, this approach is likely to dramatically limit the cross-border transfer of non-personal data, even absent actual conflict, particularly given the risk of litigation and regulatory fines embedded in the Data Act.

As noted, limiting cross-border data transfer will increase the costs of doing business for U.S. companies that utilize data processing services in many situations, including where the costs to store data in the EU exceed the costs of storing it in the United States. It may also compromise the development of artificial intelligence and other technologies that require the consolidation and processing of large volumes of data in a single location.

Further, this approach may jeopardize the safety and security of companies' data. A company may reasonably question whether EU or member state authorities can guarantee the safety and security of data stored in the EU, particularly given the other provisions in the Data Act that allow a company's competitors and EU governmental authorities to require companies to turn over such data, no matter how sensitive.

B. Challenges in Specific Sectors

The Data Act establishes a horizontal framework across all sectors, including transportation, agriculture, oil and gas, healthcare, technology, pharmaceuticals, and aerospace.[66]

The following are some key sectors that the Data Act is likely to negatively impact.

1. Automotive

Automobiles generate a great deal of data. For this reason, and because the EU is one of the United States' leading export markets for automobiles,[67] the Data Act's provisions compelling data transfer when connected products generate data will have a significant impact on the global automotive industry.

Automotive Original Equipment Manufacturers (OEMs) must ensure the safety and (cyber)-security of vehicle and their occupants. As such, it is important they can choose the best solution to allow access to the large amounts of data that modern vehicles generate and process. Moreover, not all data is accessible for or used by the car manufacturer. This could complicate automotive OEM compliance under the Data Act, depending on how requirements governing how data is to be shared. This is further complicated by streaming and storage capacities of the vehicles and the backend storage capacity of manufacturers

The definition of user in the Data Act (a natural or legal person that owns, rents or leases a product or receives a services) is particularly tricky for the auto sector as it forces automotive OEMs to provide data generated by the vehicle use to a wide range of users with whom it does not have a direct link and who may change multiple times over the lifespan of the vehicle. This would imply the need to match usage data multiple times with the different users—which may or may not be feasible.

2. Aviation

Aircraft and aircraft engines generate significant amounts of operational data while in flight. For over two decades, aircraft and engine original equipment manufacturers (OEMs) have used Aircraft Condition Monitoring Systems (ACMS) to collect this operational data and make it available to aircraft operators. The OEMs also use proprietary hardware and software to process the raw operational data in order to derive insights into the operation and functioning of the engines and other equipment. This "derived" data is proprietary information and valuable IP that the OEMs use to provide services to aircraft operators and to develop new services.

Like the aircraft and engine OEMs, aircraft operators tend to be large and sophisticated companies with substantial leverage in the market and the ability to defend their interests via contract. It is established practice in this industry for aircraft operators and OEMs to negotiate comprehensive commercial agreements at the time of sale that include data sharing agreements. These data sharing agreements typically include measures to protect trade secrets and other intellectual property, *e.g.*, by ensuring that the data holder has the exclusive right to determine when to share its proprietary data, under which conditions, and to whom. These protections are vital, because OEMs spend billions of dollars annually in research and development to develop the products and services that they offer to their customers.

In the case of the aviation sector, the Data Act is a solution in search of a problem. As a horizontal measure, it fails to take into account the particularities of the aviation sector, and it risks undoing a highly functional data-sharing regime that is already serving the interests of both data holders and users. If the Data Act imposes requirements on manufacturers that undermine their ability to protect their trade secrets and other intellectual property, the logical response will be to reduce the amount of data they collect. The result will be less innovation and higher costs, leaving the entire sector worse off than it is today.

Another unanswered question that the Data Act raises for the aviation sector in particular is how the law would apply when planes are flying internationally.

This will surely need to be spelled out in more detail and presumably be subject to numerous international agreements between companies and governments.

3. Technology

U.S. technology companies are leaders in the European data market. The Data Act targets the dominant position of U.S. technology companies in key respects.

The EU designed the gatekeeper concept to impose discriminatory rules on a handful of specific U.S. technology companies to limit their ability to compete in the EU.[68] The Data Act will also force gatekeepers to incur significant costs to modify their products and related services and face legal/compliance risk, while they are excluded from enjoying the benefits of data sharing that the Data Act purports to create.

The Data Act's provisions governing data processing service providers will have a significant negative impact on U.S. providers of cloud services, which are the leaders in the EU market. This is by design, as the Data Act's Impact Assessment specifically references the market share of the so-called U.S. "hyperscale" providers as one of the "problem drivers" the Data Act is meant to remedy.[69] The EU seeks to use the data processing service provisions in the Data Act to rebalance the EU market in favor of European companies and reduce EU dependencies on U.S.-based cloud services.

Other aspects of the EU's digital sovereignty agenda support the conclusion that the true purpose of this aspect of the Data Act is to help EU providers of data processing services better compete and take market share from U.S. providers, not to better utilize data generated in Europe for the benefit of Europeans. The proposed EU Cloud Certification Scheme (EUCS), for example, would deny "high" level security certifications to U.S. cloud suppliers due only to the location of their headquarters, regardless of whether or not they meet the technical requirements. If adopted accordingly, this lack of certification will further incentivize the switching (presumably from U.S. providers to European ones) that the Data Act is meant to facilitate.[70]

4. Pharmaceuticals and medical devices

The United States is one of the EU's main trading partners for pharmaceuticals, medical equipment, and medical supplies.[71]

Trade secrets and other intellectual property rights are the cornerstones of the pharmaceutical industry and key driving forces of innovation. Patented methodologies, clinical data, and other proprietary information reflect years of research and investment by pharmaceutical companies. Therefore, the pharmaceutical industry is particularly vulnerable to the disclosure of trade secrets and other intellectual property under the data sharing requirements of the Act.

In addition, the pharmaceutical industry relies heavily on data to accelerate the development of new drugs and improve the efficacy of clinical trials. The restrictions on international transfer of data will hinder innovation in the sector which increasingly relies on cross-border data sharing for research and development. Further, the restrictions would prevent agencies, such as the U.S. Food and Drug Administration ("FDA"), from accessing clinical trial data, which may impede product reviews and approvals. This outcome may force U.S. companies to relocate their clinical trials to third countries outside of the EU, causing companies to suffer significant relocation costs and loss of investment in the EU market.[72]

The Data Act will also impact medical devices. The Data Act's design and manufacturing requirements for products do not consider the specificities of the medical industry or account for established design and manufacturing standards in existing legislation. The EU Medical Devices Regulation and In Vitro Diagnostic Medical Regulation already specify manufacturing requirements for medical devices to ensure patient safety and security, and the data sharing requirements under the Data Act are incompatible with the sectoral requirements to ensure the cybersecurity and confidentiality of user data and the overall welfare of user (including patients).[73] U.S. businesses would also have to ensure compliance with the FDA's device regulations, which are likely to be in conflict with requirements imposed by the Data Act in its current form.

Especially coming out of a global pandemic where international data sharing was essential for the research, development, and implementation of vaccines, therapeutics, and drugs to counter COVID-19 at record speed—now is exactly the wrong time to impose new restrictions on data flows in the health sector.

5. Financial services

The financial services industry is one of the most data-reliant sectors in the economy. Data sharing is an industry norm and financial institutions regularly enter into complex data sharing agreements.
In the business-to-business context, these complex agreements will be disrupted by requirements under the Data Act limiting contractual freedom, which will also restrict the ability of financial institutions to negotiate new contractual arrangements to address novel issues such as FinTech.

It is also unclear how the Data Act interacts with sector-specific guidelines and regulations. For example, the Second Payment Services Directive enables customers and SMEs to share their current account information securely with other third-party providers.[74]
Moreover, since 2018, the EU has promoted the use of standard contractual clauses for financial services outsourcing to cloud services and the EU has also introduced various guidelines for cloud outsourcing.[75] Nevertheless, the Data Act does not provide any clear guidance as to how its regulation of cloud service providers will interact with these parallel initiatives.

Finally, the restrictions on international transfer of non-personal data under the Data Act will place a unique strain on the financial industry. Cross-border data flows are the lifeblood of global financial markets. Barriers under the Data Act to the international transfer of data conflict with the daily necessity of international data sharing in the financial sector. Any data localization requirements will hinder global operations of. financial services companies, placing new strain on our economies at a time where the economic recovery remains fragile.

III. The Data Act is Inconsistent With Key WTO Rules

It is uncertain how the EU will implement numerous aspects of the Data Act, should it become law. Nonetheless, it is already apparent that the Data Act raises serious concerns under international trade rules, including the rules of the World Trade Organization ("WTO"). These concerns implicate several WTO agreements, including the General Agreement on Tariffs and Trade 1994 ("GATT 1994"); the Agreement on Trade-Related Aspects of Intellectual Property Rights (the "TRIPS Agreement"); the Agreement on Technical Barriers to Trade (the "TBT Agreement"); and the General Agreement on Trade in Services ("GATS"). The following are some of the key areas of concern.[76]

A. GATT 1994

The GATT 1994 is the core WTO agreement establishing disciplines on trade in goods, including the national treatment obligation set out in GATT Article III, which generally prohibits nationality-based discrimination against imported products.

Article III:4 of the GATT 1994 obliges WTO Members to treat imported products "no less favorably" than like domestic products.[77] It is well-established that Article III:4 obliges WTO Members to provide conditions of competition no less favorable to imported products than to like domestic products, and that a measure will breach this obligation if it modifies such conditions to the detriment of the imported products.[78] It is also well-established that the application of formally identical legal provisions may in practice accord less favorable treatment to imported products.[79] Article III:4 covers not only measures that directly regulate the sale of domestic and imported products, but also measures that create incentives or disincentives with respect to the sale, offering for sale, purchase and use of imported products.[80]

As discussed above, the Data Act prohibits data transfers to companies designated as "gatekeepers" under the Digital Markets Act. If a gatekeeper manufactures products subject to the Act–*e.g.*, smart home devices–it may not access data generated by other products or related services under the Data Act, *even where a user of such products or services wishes to grant a gatekeeper such access*. This prohibition is in tension with Article III:4, because it will undermine the competitiveness of imported products manufactured by gatekeepers–most if not all of which will be U.S. companies–relative to like domestic products.[81]

B. TRIPS

The TRIPS Agreement establishes minimum standards of protection for intellectual property. TRIPS Article 39.2 addresses the protection of undisclosed information, *i.e.*, trade secrets. Specifically, Members must ensure that a person lawfully in control of undisclosed information has the possibility of preventing it from being disclosed to, acquired by, or used by others without his or her consent in a manner contrary to honest commercial practices.[82]

The Data Act is in tension with this obligation, because (1) the Data Act *expressly requires* data holders in certain circumstances to transfer trade secrets to users of their products and third parties–including their direct competitors; (2) the protections for such trade secrets in the Data Act are weak and ineffective; and (3) the Data Act *does not* prevent users or data recipients from exploiting data they receive for various purposes, including developing competing services.[83]

C. TBT Agreement

The TBT Agreement establishes rules meant to ensure that technical regulations, standards, and conformity assessment procedures are non-discriminatory and do not create unnecessary obstacles to trade.[84] Article 2.1 of the TBT Agreement contains a national treatment obligation that prohibits technical regulations that discriminate between domestic and imported like products.[85]

The gatekeeper provisions in the Data Act will likely breach Article 2.1 of the TBT Agreement for the same reason that they will likely breach GATT Article III:4: they will accord less favorable treatment to imported products that generate data and are manufactured by gatekeepers than to like products manufactured by EU companies that are not gatekeepers.

D. GATS

The GATS is the core WTO agreement that liberalizes trade in services. Similar to the GATT 1994, the GATS includes a national treatment obligation that requires WTO Members to treat foreign services and service suppliers "no less favorably" than like domestic services and service suppliers.[86] Unlike the GATT obligation, the GATS national treatment obligation applies on a "positive list" basis solely to the sectors and "modes of supply" that a WTO Member has inscribed in its GATS schedule of commitments.[87]

The EU has undertaken national treatment commitments in numerous service sectors and modes of supply that the Data Act would implicate. For example, the EU and most of its Member States have undertaken full commitments for national treatment in modes 1-3 for "*Computer and Related Services*" ("CRS").[88] The CRS sector is further broken down into several subsectors relevant to the Data Act, including "software implementation services," "data processing services," "data base services," and "other" computer services.[89] Of critical importance for a GATS assessment of the Data Act, the EU is on the record at the WTO that cloud computing falls within the scope of CRS.[90]

Several aspects of the Data Act are in tension with the EU's GATS national treatment obligations. The following are some key examples.

1. Information-sharing requirements

In a wide variety of sectors, companies will be required to transfer trade secrets and other commercial information to their competitors, who can use the information to develop competing services. In some sectors, this may modify competitive conditions to the detriment of U.S. services and service suppliers.

2. Restrictions on cross-border transfers

As discussed above, the Data Act requires providers of data processing services to take all reasonable steps to prevent the international transfer of non-personal data held in the EU where such transfer would create a conflict with the law of the EU or its member states.[91] The Data Act does not explain the circumstances under which a transfer would have this effect, however. One example would be Article 31 of the Data Governance Act, which restricts international transfers in which the right to re-use was granted. Given this lack of explanation, it is notable that the Commission's Impact Assessment on the Data Act specifically references Executive Order 12333, Section 702 of the Foreign Intelligence Surveillance Act (FISA), and the U.S. CLOUD Act as examples of foreign laws with extraterritorial effect that have "raised concerns among European citizens and businesses."[92]

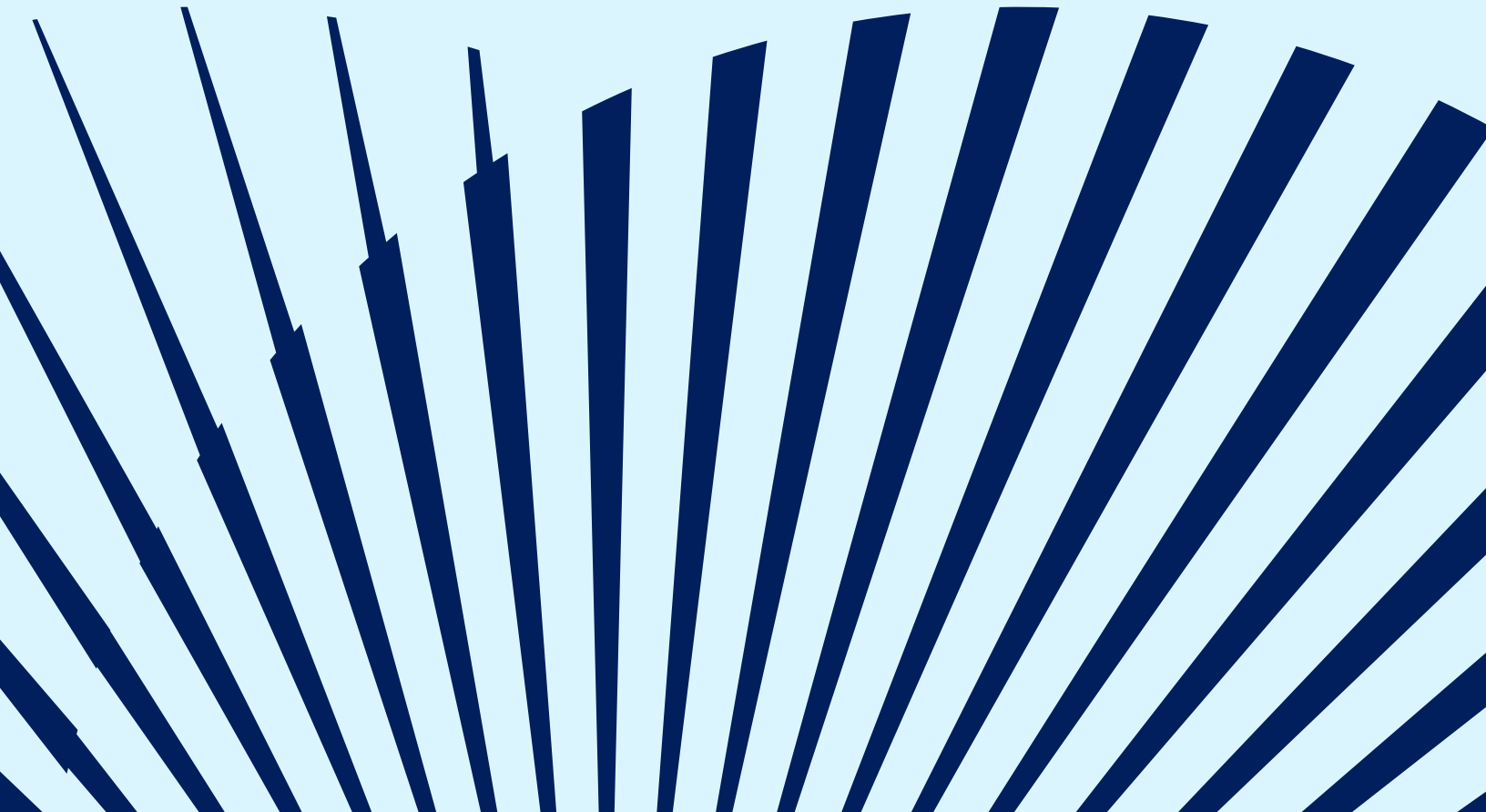
In the *Schrems II* decision (which involved the GDPR), the European Court of Justice (CJEU) pointed to Executive Order 12333 and Section 702 of FISA as part of its rationale for invalidating the Privacy Shield.[93] In light of this history, it cannot be dismissed that the EU and/or the CJEU would interpret the Data Act's provisions on international transfers in such a way as to effectively prohibit U.S. providers of data processing services from transferring non-personal EU data to the United States for processing and storage.[94] If the EU were to take this step, there would be a strong argument for a breach of the EU's national treatment obligation, because a measure that prohibits a foreign company from supplying a committed service that a domestic company is permitted to supply–which would effectively be the case here–is inconsistent with national treatment.[95]

In addition, even if the EU were not to interpret the Data Act in this manner, it would still require foreign providers of data processing services to conduct resource-intensive risk assessments before they would be able to transfer EU non-personal data to third countries, including the United States. These additional costs—which EU-based cloud service suppliers such as Deutsche Telekom, OVHcloud, SAP, and Orange would not incur—are likely to modify competition conditions in the EU market to the detriment of foreign providers, contrary to GATS requirements.

3. Restrictions on data access by gatekeepers

The Data Act's prohibition on data transfers to companies designated as "gatekeepers" under the Digital Markets Act is another provision that arguably violates the EU's GATS national treatment commitments on a *de facto* basis. This is because the prohibition will modify competitive conditions in the EU market to the detriment of gatekeepers, which are disproportionately foreign (and American).

As an initial matter, it is indisputable that these aspects of the Data Act will modify competitive conditions in the EU market, as this is one of their express purposes.[96] Further, it is also indisputable that the provisions will modify competitive conditions to the detriment of gatekeepers, because they will require gatekeepers to share data with their competitors to use in the development of new services, while prohibiting gatekeepers from receiving such data for the same purposes.[97] Finally, as discussed above, it is likely that gatekeepers will be disproportionately foreign, because the EU designed the gatekeeper criteria in the Digital Markets Act to cover large U.S. platforms while excluding a maximum number of European platforms that provide like services.



Conclusion

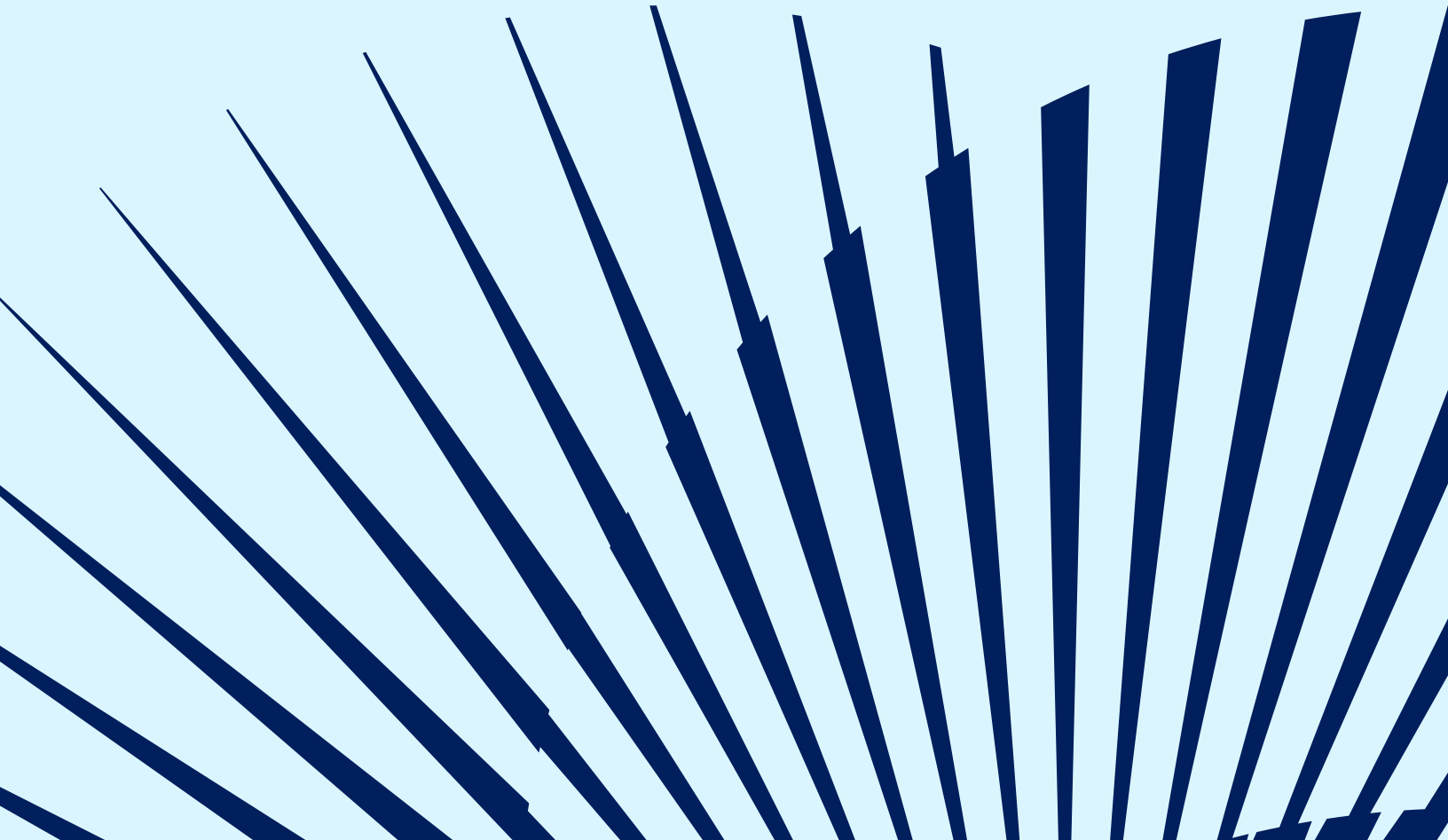
As noted at the outset of this paper, its purpose is to alert policymakers at home and abroad to the potential consequences—whether intended or otherwise—of the Data Act, as initially put forward by the European Commission. These concerns are broadly held across sectors, reflecting the vast reach of this proposal. Indeed, any U.S. company that manufactures products sold in Europe that generate data, provides services in Europe allowing such products to perform their functions, provides data processing services in Europe, or is otherwise considered a "data holder" in Europe, could experience direct economic harm, with a potential chilling effect on investment and innovation.

Moreover, any European company with operations in the United States may be adversely impacted by new restrictions on international data flows for industrial data, which could undermine their future investments in the United States. Perhaps most concerningly, without sufficient safeguards for trade secrets or other intellectual property, companies may be forcibly compelled to hand over their hard-won and valuable data sets to their competition—including to state-owned enterprises from China and other adversarial nations. These outcomes need to be avoided in order to prevent both a loss of economic competitiveness and potential serious threats to our national security.

To be clear, unlocking the potential for data sharing across the economy is critical to powering the digital transformation of businesses and organizations of all sizes. We share the Commission's desire to see a connected and competitive digital economy in Europe. However, governments must strike an appropriate balance between bolstering data sharing, facilitating the privacy and safety of users, and enabling innovation through strong protections for intellectual property and trade secrets. The EU Data Act fails to accomplish these goals. Indeed, mandated data sharing between businesses and governments, and between businesses and their competitors, very likely represents significant breaches of international trade commitments long championed by both the United States and the European Union.

Given these concerns, we urge the U.S. government to move quickly and utilize all available options to dissuade the EU from bringing the measure into law, at least in its current form. Fortunately, there is still some time. European policymakers are currently considering revisions to the Data Act, including potential compromises that would address some of the concerns raised by stakeholders. With this window of opportunity closing, it is incumbent upon U.S. policymakers to urgently engage their European counterparts to develop an alternative approach to regulating data in the global digital economy. Such an approach must prioritize contractual freedom, voluntary data sharing, and non-discrimination.

Finally, it is important to get the policy framework for data sharing right in the EU context. Otherwise, we will quickly see similar measures adopted outside of Europe, including in countries that do not share our transatlantic values of free enterprise, freedom of expression, and the rule of law. Mandated data sharing practices, in those economies could prove to be even more harmful than the challenges created by the EU Data Act.



Endnotes

1 Proposal for a Regulation of the European Parliament and of Council on Harmonized Rules on Fair Access to and Use of Data ("Data Act"), COM/2022/68 (Feb. 22, 2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0068.

2 U.S.-EU Trade Relations, Congressional Research Services (June 3, 2022), 1-4, https://crsreports.congress.gov/product/pdf/R/R47095#:~:text=In%202021%2C%20the%20EU%20accounted,supplier%20of%20goods%2C%20after%20China.

3 Sweden, the holder of the Presidency of the Council of Europe during the first half of 2023, unveiled the most recent proposal on January 24, 2023. See Luca Bertuzzi, Swedish Presidency Tries to Close in on the Data Act, Euractiv.com (Jan. 25, 2023), https://www.euractiv.com/section/data-privacy/news/swedish-presidency-tries-to-close-in-on-the-data-act/.

4 Data Act, Explanatory Memorandum, p. 1.

5 Data Act, Art. 4(1).

6 Data Act, Art. 3(2).

7 Data Act, Art. 4(6). Further, the Data Act prohibits data holders from using generated data to gain insights about the economic position, assets, and production methods of the user that could "undermine the commercial position of the user" in the relevant market. Id. at Recital 25.

8 Data Act, Art. 4(4).

9 Data Act, Recital 35.

10 Data Act, Art. 3(1).

11 Data Act, Art. 5.

12 Data Act, recital 29.

13 Data Act, Arts. 8(1), 9(1).

14 Data Act, Art. 11(1).

15 Data Act, Art. 10.

16 Data Act, Art. 6(2).

17 Data Act, Art. 15.

18 Data Act, Art. 15.

19 Data Act, Arts. 18, 31.

20 Data Act, Art. 1 (defining "data processing service" as, subject to certain exceptions, a "digital service ... provided to a customer, which enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralized, distributed or highly distributed nature").

21 Data Act, Art. 23(1).

22 Data Act, Art. 26(1).

23 Data Act, Art. 26(3).

24 Data Act, Art. 29(1).

25 Data Act, Art. 27(1).

26 Data Act, Art. 27(2).

27 Data Act, Art. 27(5).

28 European Commission, Data Act: Commission proposes measures for a fair and innovative data economy (Feb. 23, 2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

29 See Data Act, Arts. 4(1), 9(3).

30 See Data Act, Arts. 4(4), 6(2)(e).

31 Data Act, Art. 6(2)(c).

32 Data Act, Art. 11(3).

33 Data Act, Art. 23(1).

34 Data Act, Arts. 26(1), 26(3), 29(1).

35 Data Act, Art. 4(3).

36 Data Act, Art. 4(3).

37 Data Art. Art. 5(8). A separate provision in the Data Act–Article 8(6)–could potentially provide some measure of protection to trade secrets in the context of data transfers between data holders and third-party data recipients, but the language is vague and unclear. See id. at Art. 8(6) ("Unless otherwise provided by Union law, including Article 6 of this Regulation, or by national legislation implementing Union law, an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets within the meaning of Directive (EU) 2016/943.").

38 Data Act, Art. 11(1).

39 Data Act, Art. 13(1).

40 Data Act, Art. 19(2); see id. at Art. 17(2)(c) ("A request for data [by a public body or EU institution] shall . . . respect the legitimate aims of the data holder, taking into account the protection of trade secrets and the cost and effort required to make the data available[.]").

41 Data Act, Art. 15(c) (allowing EU governmental authorities to compel data transfer "where the lack of available data prevents the [governmental authority] from fulfilling a specific task in the public interest that has been explicitly provided by law; and (1) the [governmental authority] has been unable to obtain such data by alternative means ...; or (2) obtaining the data in line with the procedure laid down in [Chapter V of the Data Act] would substantively reduce the administrative burden for data holders or other enterprises").

42 Data Act, Art. 19(2).

43 Data Act., Art. 4(1) (requiring data holders to transfer data to users without compensation); id. at Art. 9(3) (providing that the EU or EU Member States may exclude compensation to data holders transferring data to data recipients).

44 The preamble to the Data Act states that intellectual property rights will be respected. See Data Act, Recital 23. However, this is not reflected in the provisions of the Data Act.

45 See Data Act, Art. 35 (disapplying sui generis intellectual property right with respect to databases containing data generated by the use of a product or related service).

46 In the standard essential patent context, a FRAND commitment is the result of a voluntary agreement to contribute a patent to a standard. Here, the FRAND commitment is not the result of voluntary agreement, but rather a government mandate.

47 Josef Drexl et al. Position Statement of Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonized rules on fair access to and use of data (Data Act), Max Plank Institute for Innovation and Competition, 38 (May 25, 2022), https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/Position_Statement_MPI_Data_Act_Formal__13.06.2022.pdf.

48 Data Act, Art. 10(2).

49 Data Act, Art. 10(8).

50 Data Act, Arts. 10(5), 10(9).

51 Data Act, Recital 41.

52 Data Act, Arts. 5 and 8.

53 Data Act, Recital 17.

54 Data Act, Art. 1.

55 Data Act, Art. 33(3).

56 Data Act, Art. 33(4).

57 See https://www.enforcementtracker.com/.

58 Data Act, Art. 26(4).

59 Data Act, Arts. 29(1).

60 Data Act, Art. 23(2), Art. 24(1).

61 Cloud application services are typically integrated within a customer's IT system and implemented over a 6-to-18-month period. See Workday, Response to the European Commission's Request for Feedback on the Proposed Data Act, 3 (May 13, 2022).

62 As discussed below, the Data Act's negative impact on U.S. cloud companies appears to be intentional.

63 This topic has been discussed by the Council and the European Parliament, and it seems likely that some changes may be adopted—however their impact is still impossible to ascertain.

64 Data Act, Art. 6(2)(b) (incorporating definition of "profiling" in Article 4(4) of Regulation (EU) 2016/679: "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.").

65 Data Act, Art. 27(1).

66 Study to support an Impact Assessment on enhancing the use of data in Europe, European Commission, 178, (Feb. 23, 2022), https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act.

67 For example, the EU accounts for 19% of the total value of U.S. automobile exports. See Fact sheet: EU-US automobile trade, acea (Mar. 18, 2019), https://www.acea.auto/fact/fact-sheet-eu-us-automobile-trade/.

68 There is substantial evidence in the public record supporting the conclusion that the EU designed the "gatekeeper" category to target specific U.S. companies, while excluding a maximum number of European platforms that provide like services. For example, Andreas Schwab, the European Parliament's rapporteur for the Digital Markets Act, argued that in designating companies as gatekeepers under the DMA, the EU should focus on the "biggest problems," i.e., Google, Apple, Amazon, Facebook, and Microsoft. "Let's focus first on the biggest problems, on the biggest bottlenecks. Let's go down the line–one, two, three, four, five–and maybe six with Alibaba," Schwab said. "But let's not start with number 7 to include a European gatekeeper just to please Biden." See Javier Espinoza, "EU should focus on top 5 tech companies, says leading MEP," Financial Times (May 31, 2021).

69 See, e.g., Impact Assessment at 24 and n. 113 (specifically referencing the U.S. suppliers Amazon, Microsoft and Google in the footnote); id. at 25 (asserting that "poor switchability" strengthens the dependence of European cloud users on non-EU service providers).

70 See, e.g., Kenneth Propp, European Cybersecurity Regulation Takes A Sovereign Turn, Atlantic Council (Sept. 13, 2022), https://www.crossborderdataforum.org/european-cybersecurity-regulation-takes-a-sovereign-turn/.

71 In 2019, the United States accounted for 27 percent of EU imports of pharmaceuticals; 35 percent of EU imports of medical equipment; and 44 percent of EU imports of medical supplies. EU imports and exports of medical equipment, European Parliament, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649387/EPRS_BRI(2020)649387_EN.pdf.

72 Rozi Kepes et al. The importance of cross-border data flows: An economic assessment of restrictions on extra-EU data transfers, AG Analysis Group, https://about.fb.com/wp-content/uploads/2021/06/The-Importance-of-Cross-Border-Data-Flows.pdf; see also Heather Messick, How a European Data Law is Impacting FDA, FDA (Aug. 9, 2022), https://www.fda.gov/international-programs/global-perspective/how-european-data-law-impacting-fda.

73 MTE position on the Proposal on harmonized rules on fair access and use of Data (Data Act), MedTech Europe (Nov. 4, 2022), https://www.medtecheurope.org/wp-content/uploads/2022/11/221104-data-act-position-paper.pdf. As noted by MedTech Europe, Data Act requirements do not consider the particularities of medical devices which may be unable to support increased data sharing or hosting without further modification. These modifications may harm patient welfare where certain implantable medical devices are required to be frequently replaced to comply with the Data Act's data sharing and storage requirements.

74 Study to support an Impact Assessment on enhancing the use of data in Europe, at para. 4.2.3.1.1.

75 European Commission, Directorate-General for Justice and Consumers, Graux, H., Somers, G., Van Camp, S., et al., Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights : final report, Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2838/174720; *see also Communication From the Commission: Fintech Action Plan: For a more competitive and innovative European financial sector,* COM (2018) final 109 (Aug. 3, 2018), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0109&rid=15.

76 The Data Act may violate other international rules–including international investment rules–depending on how the measure is implemented. For example, depending on the role that EU Member States play in implementation, the measure could violate one of the 9 bilateral investment treaties that the United States has with EU Member States (Bulgaria, Croatia, the Czech Republic, Estonia, Latvia, Lithuania, Poland, Romania, and Slovakia).

77 GATT Art. III:4.

78 See, e.g., Appellate Body Report, Korea–Various Measures on Beef, para. 135.

79 Panel Report, Dominican Republic–Import and Sale of Cigarettes, para. 7.182.

80 Panel Report, China–Publications and Audiovisual Products, para. 7.1450.

81 As stated above, there is substantial evidence in the public record supporting the conclusion that the EU designed the "gatekeeper" category to target specific U.S. companies while excluding a maximum number of European platforms that provide like services.

82 TRIPS, Art. 39.2. To qualify as "undisclosed information," the information must (1) be secret; (2) have commercial value because it is secret; and (3) have been subject to reasonable steps by the person lawfully in control of the information, to keep it secret. Id.

83 The same TRIPS issue arises with respect to the implicit requirement in the Data Act that an incumbent cloud service provider transfer trade secrets to a new cloud service supplier, to the extent necessary to ensure functional equivalence for the customer switching service providers.

84 The Data Act is a "technical regulation" within the meaning of the TBT Agreement because it establishes mandatory characteristics for certain products. See TBT Agreement, Annex 1.1 (defining the term "technical regulation"); Data Act, Art. 3(1) ("Products shall be designed and manufactured . . . in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user").

85 TBT Agreement, Art. 2.1. The provision also includes a most-favored nation (MFN) obligation.

86 GATS, Art. XVII.

87 There are four "modes" of supply. Cross-border supply is "mode 1"; supply to a foreign national who has traveled to the supplying country (referred to as "consumption abroad") is "mode 2"; supply via a commercial presence in the foreign country is "mode 3"; and supply by an individual to service consumers in the foreign country (referred to as "presence of natural persons") is "mode 4."

88 Trade in Services - European Union - Schedule of specific commitments, WTO Document GATS/SC/157 (May 7, 2019), 58-64. For "software implementation services," "data processing services," "data base services," and "other computer services," Malta's concessions are "unbound." Cyprus, Hungary, and Poland's concessions are "unbound" for "other computer services."

89 Trade in Services - European Union - Schedule of specific commitments, WTO Document GATS/SC/157 (May 7, 2019), 58-64.

90 See, e.g., WTO Council for Trade in Services, Report of the Meeting Held on 18 March 2015: Note by the Secretariat, S/C/M/122 (May 1, 2015), https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/M122.pdf&Open=True.

91 Data Act, Art. 27.1.

92 See Impact Assessment at 20 and n. 97-98.

93 See Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems EU:C:2020:559 (Schrems II). Although the United States and the EU have negotiated a new EU-U.S. Data Privacy Framework as a successor to the Privacy Shield, the new agreement only covers personal data. See, e.g., European Commission, Questions & Answers: EU-U.S. Data Privacy Framework, draft adequacy decision (Dec. 13, 2022).

94 Luca Bertuzzi, Data Act: The EU makes its next move for industrial data, IAPP (Feb. 23, 2022), https://iapp.org/news/a/data-act-the-eu-makes-its-next-move-for-industrial-data/

95 See, e.g., Panel Report, China–Publications and Audiovisual Products, para. 7.1311 (finding the Chinese measures at issue to be inconsistent with China's national treatment commitments because they prohibited service suppliers of other Members from engaging in the supply of electronic distribution of sound recordings, while like domestic service suppliers were not similarly prohibited).

96 See, e.g., Data Act, recitals 28 and 29.

97 Data Act, Art. 5(2); see also id., recital 36 (discussing the restrictions that the DMA and the proposed measure impose on gatekeepers).