Seton Hall University
eRepository @ Seton Hall

Student Works | Seton Hall Law

2025

A Holistic Overview of the Data Act, Its Implications on the Economy and Interplay with the GDPR

Mary A. Mikhail

Follow this and additional works at: https://scholarship.shu.edu/student_scholarship

 Part of the Law Commons

I. Introduction

The data you generate, whether through Google searches, everyday purchases, or even conversations with your Amazon Alexa, is priceless. An estimated 328.77 million terabytes of data are generated every day.[1] Data is essential information gathered from everyday activities that, when analyzed, can help society make better decisions and improve processes and inefficiencies.[2] Employing the data we generate is essential to better company performance and improve overall customer experiences.[3] The data generated by customers helps companies track consumer behavior, to learn about patterns or issues related to customer satisfaction. By allowing establishments to access and study consumer data, our quality of life can be improved.[4] Therefore, a lack of available data inhibits our ability to effectively solve problems and ameliorate our technologically driven society. Although increasing the availability and value of generated data can be incredibly beneficial, a restricted market view tailored towards a single market of data within one Union may not be the best approach towards achieving greater access to essential data.

The European Union's (EU) latest data privacy regulation, the Data Act, [5] is a massive and precarious step forward towards a unified data market within the Union. This paper argues that the European Commission must take a small step back and reevaluate the Data Act's requirements in order to better achieve a unified data market. The Act was enacted on January 11, 2024 and will

[1] Fabio Duarte, *Amount of Data Created Daily*, Exploding Topics, Dec. 13, 2023, at 1, https://explodingtopics.com/blog/data-generated-per-day - :~:text=According to the latest estimates,or 0.33 zettabytes every day.
[2] Duarte, *supra* note 1 at 1.
[3] *Id.*
[4] Dan Price, *How Much Data is Produced Every Day*, Cloud Tweaks, Mar. 17, 2015, at 1, https://cloudtweaks.com/2015/03/how-much-data-is-produced-every-day/#:~:text=A.,a%20staggering%2018%20zeros!).
[5] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data and amending Regulation EU 2017/2394 and Directive 2020/1828 [hereinafter "Data Act"].

be applicable in September 2025.[6] The Act hugely disadvantages US-based companies that generally hold and control a large portion of EU data.[7] These disadvantages may ultimately lead to a single EU data market, which is one of the main objectives of the Act, but may also harm EU-based companies in turn.[8] The Act seemingly seeks to make more data available within Europe by creating rigid protection laws for the access and utilization of consumer-generated data.[9] Although this may overall be helpful to protect consumer information, the Act punishes foreign countries, like the US, by requiring disclosure of intricate trade secrets in an effort to make EU companies more competitive.[10] This paper will study the main objective of the Data Act in Section 2, discuss the economic implications of the Act on EU and US companies in Section 3 and explore the Act's interplay with the GDPR in Section 4.

II. Overview of the Data Act

Although data generation has expanded tremendously due to the recent boom in technology, its use has remained relatively low.[11] This is because only a handful of corporations have access to large quantities of data.[12] Different economic priorities and technological hurdles are the main reasons for this offset in data use.[13]

The lack of data access has also been blamed on cloudy data rights, restricted access to reputable cloud-servicing agents, disproportionate bargaining power in negotiations, and overall

---

[6] European Commission, *Shaping Europe's Digital Future,* at 3, https://digital-strategy.ec.europa.eu/en/node/10725/printable/pdf.
[7] Meredith Broadbent, *The Long Arm of European Tech Regulation Continues*, Center for Strategic & International Studies, June 2023, at 3, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-06/230629_Broadbent_Data_Act.pdf?VersionId=pCFa4JgreCVhjF.tfYA8Dzp3GRJzI0IL.
[8] Broadbent, *supra* note 7 at 2.
[9] *Id.* at 3.
[10] *Id.*
[11] Data Act, *supra* note 5, Preamble (2), at 1.
[12] *Id.*
[13] *Id.*

insufficient collaborative data available in the EU.[14] Vague data rights cast a cloud not only on who has access to data generated from electronic products but also on who can use them.[15] Reputable cloud-servicing agents have obstacles that make it tough for just anyone to be able to switch into and use their services. Small and medium-sized enterprises (SMEs) struggle to maintain equal bargaining power in negotiations with larger corporations, making it harder to obtain and share data through equitable data-sharing agreements.[16] Lastly, large sums of data that are gathered from distinct areas or countries are not easily combined with local data, making it harder to use collaborative data within the EU.[17]

In 2022, the European Commission proposed the Data Act,[18] which was later adopted by Council in 2023.[19] The Act is authorized by Article 114 of the Treaty on the Functioning of the European Union (TFEU).[20]

The Data Act's main objective is to ensure fair access and use of data throughout the EU.[21] By requiring companies to allow their users' data to be accessed and reused, data will be made more available and help encourage a competitive market.[22] Access to data will allow manufacturers to not only understand consumers but help solve their issues and advance the quality of products and services provided to them.[23]

---

[14] *Id.*
[15] Data Act Questions and Answers, (June 28, 2023) [hereinafter "Data Act Questions and Answers"].
[16] *Id.*
[17] *Id.*
[18] Commission Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access and to and use of data (Data Act), COM (2022) 68 final (Feb. 23, 2022).
[19] Hope Anderson, *The Data Act – the EU's bid to "ensure fairness in the digital environment and a competitive data market" – has been adopted*, Nov. 30, 2023, at 1, https://www.whitecase.com/insight-alert/data-act-eus-bid-ensure-fairness-digital-environment-and-competitive-data-market-has. *See also* Data Act, *supra* note 5.
[20] Data Act, *supra* note 5, Preamble. Article 114 concerns the European Commission's efforts to protect the environment, consumer, as well as their health and safety. Consolidated Version of the Treaty on the Functioning of the European Union art. 114, 2012 O.J. C 326/47, at 3 [hereinafter TFEU].
[21] Council Press Release, IP/23/932 (Nov. 27, 2023).
[22] *Id.*
[23] *Id.*

The Data Act homes in on data generated specifically from connected devices. A connected product is any device that "obtains, generates or collects data" about its users and can convey that data.[24] Consumers of typical household or personal devices will be able to access their data which was previously held only by their manufacturers or service providers.[25] Additionally, the Act distinguishes between data collected through a connected product's use versus traditional product data.[26] While the Act pushes for the sharing and use of data, the Data Act claims to establish protections against the unauthorized access and abuse of trade secrets, as well as processes for dispute resolution, which will be discussed more in-depth in Section 3.[27]

The Data Act, enacted after the Database Directive, [28] was intended to clear up various ambiguities identified in the Database Directive.[29] In 1996, the Council adopted the Database Directive during a time when technology was rapidly excelling.[30] As the growth of technology and internet use boomed across the EU, a need developed for legislation that established and protected the rights of both data generators and data holders, while also putting pressure on creating both a competitive digital market and one set of laws governing the rights of data holders across the EU.[31] The Database Directive was designed to protect investments in intellectual property for the creation of databases through the *sui generis* right.[32] The *sui generis* right protects "substantial investment" made in database creation and protects against unlawful takings or use of the content

[24] Data Act, *supra* note 5, art. 2(5), at 34.
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] Council Directive 96/9/EC of the European Parliament and of the Council on the Legal Protection of Databases, 1996 O.J. L 158/77 [hereinafter "Database Directive"].
[29] Data Act Questions and Answers, *supra* note 15.
[30] European Commission, *Study to Support an Impact Assessment for the Review of the Database Directive Final Report,* Publications Office of the European Union, Feb. 14, 2022, at 24, https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act. [hereinafter "Impact Assessment Report"].
[31] Impact Assessment Report, *supra* note 30 at 24.
[32] Database Directive, *supra* note 28, art. 3 and art. 7, at 25.

for 15 years.[33] Criticisms on the Data Act's incorporation of the *sui generis* right, or rather a lack thereof, will be addressed in Section 3.

The Database Directive's weaknesses seem to be the cited cause of many of the issues which led to the proposal of the Data Act.[34] Critics argue that the Database Directive has not had much of an effect or contribution to the EU's digital economy.[35] As previously mentioned, lack of clarity as to who has access to data generated from electronic products and who can use it has been a cause of decreased use of data throughout the EU.[36]

Data generated through connected products are held by data holders who may not necessarily be considered owners of the data, but can still control who has access to the data and where it is allowed to go.[37] This is especially troubling because, without an established framework regarding who has the right to control the data, data holders are put at an advantage over third parties and other companies in need of the data when bargaining for data sharing agreements.[38] Unequal bargaining power not only hurts companies economically but also leads to unrealized use of valuable data, ultimately harming potentially valuable innovation.[39]

The intricacy of data rights and obligations has opened the conversation to promoting a single data market in the EU, primarily an open data market.[40] An open data market is expected to cause economic and technological growth in the EU.[41] The Data Act's Impact Assessment for review of the Database Directive specifically attributes growth in AI, robotics, and automation

---

[33] *Id.*
[34] *Id.*
[35] THOMAS STREINZ, *THE EVOLUTION OF EUROPEAN DATA LAW*, at 918 (Paul Craig & Gráinne de Búrca eds., 3rd ed. 2021).
[36] Data Act Questions and Answers, *supra* note 15.
[37] Impact Assessment Report, *supra* note 30, at 46.
[38] *Id.*
[39] *Id.*
[40] *Id.* at 33.
[41] *Id.*

within an open data market.[42] An open data market concept is exactly what led to the proposal of the Data Act.[43] The EU's need for greater data sources and sharing will stimulate a more competitive market for businesses by creating a more level playing field and will ultimately push for innovation and advancement.[44]

One major example of how an open data market can benefit society is the process of data sharing during the height of COVID-19.[45] In an effort to support each other and collaborate as a society on solutions to impede the spread of the virus, data holders transferred over eighty thousand pieces of written work and research data to scientists and pharmaceutical companies.[46] This sharing of data enhanced our understanding of the virus and led to improved prevention and control over the spread of the virus.[47]

The intricate requirements of the Data Act require thoughtful enforcement. The Act generally places enforcement responsibilities on Member States.[48] Member States are authorized to delegate to the "competent authorities" the responsibility of enforcing the Act.[49] If one or more authorities are delegated, a data coordinator must also be set.[50] Data coordinators are helpful in cases where authorities may not know what the best course of action is when dealing with authorities from another Member State.[51] Data coordinators are regarded as the "single point of contact" for issues arising under the Act.[52] Authorities are required to work with each other and share the ability to access information on data processing organizations in order to adequately

[42] *Id.*
[43] Council Press Release, *supra* note 21, IP/23/932 (Nov. 27, 2023).
[44] *Id.*
[45] Impact Assessment Report, *supra* note 30, at 33.
[46] *Id.*
[47] *Id.*
[48] Data Act, *supra* note 5, Preamble (107) at 29.
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.*

carry out their duties.[53] Authorities in one Member State must also assist other authorities in other Member States if necessary.[54]

Penalties are incurred if entities violate the Act.[55] These penalties may include fines, warnings, and even injunctions to require organizations to follow the Act's requirements.[56] If a violation has occurred, authorities are tasked with minimizing the effect of the violation while an investigation is underway.[57] Authorities are directed to "take into account, inter alia the nature, gravity, scale and duration of the infringement in view of the public interest at stake, the scale and kind of activities carried out, and the economic capacity of the infringing party."[58] Similar to double jeopardy, the Act warns of punishing entities for the same violation more than once under the principle *ne bis in idem*.[59] Authorities are expected to communicate with coordinators regarding any infringements in order to prevent double penalization.[60]

The Data Act was proposed in hopes of ensuring the fair access and use of data throughout the EU.[61] The goals of making data more accessible and helping encourage a competitive market were large forces behind the Commission's proposal.[62] Although the Act's good intentions seem promising, the actual application of the regulation falls short in some respects.

III. Economic Implications

Although the Act claims to be tailored towards aiding EU companies and disadvantaging US-based companies within the EU data market, EU businesses have expressed real concerns

[53] *Id.*
[54] *Id.*
[55] Data Act, *supra* note 5, Preamble (109) at 29.
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] Council Press Release, *supra* note 21, IP/23/932 (Nov. 27, 2023).
[62] Data Act Questions and Answers, *supra* note 15.

surrounding major requirements under the Act. This section will discuss multiple economic implications both US and EU companies might face in consequence to the Act's provisions.

Companies based in the US face challenges from the adoption of the Data Act.[63] The US Chamber of Commerce published a report on March 2, 2023, giving an overview of the Data Act as well as comments on the Act's weaknesses.[64] In its report, the Chamber of Commerce emphasized the importance of increasing competition and establishing a fair single market surrounding data sharing in the EU but found that the Act was not the correct way to achieve such.[65] Specifically, the Act will not promote competition amongst companies; rather, it will "penalize competition on the merits and chill investment and innovation".[66] Hinting toward an issue more related to competition law, the report argues that the Act punishes companies who have expanded business in the EU and have formulated mass amounts of data within the Union, solely because the Commission hypothesizes the Act will stimulate the use of data.[67]

A. Trade Secret and Intellectual Property Concerns

The Chamber of Commerce's major concern with the sharing of trade secrets lies in Article 4 of the Data Act.[68] Section 6 of Article 4 states,

> Trade secrets shall be preserved and shall be disclosed only where the data holder and the user take all necessary measures prior to the disclosure to preserve their confidentiality in particular regarding third parties. The data holder . . . . shall agree with the user proportionate technical and organizational measures necessary to preserve the confidentiality of the shared data, in particular in relation to third parties, such as model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct.[69]

---

[63] Jordan G. Heiber, Garret Workman, *The EU Data Act: A Misguided Policy*, US Chamber of Commerce EU Data Act Report, Mar. 2, 2023, at 3, https://www.uschamber.com/international/the-eu-data-act-a-misguided-policy [hereinafter "Chamber of Commerce Report"].
[64] Chamber of Commerce Report, *supra* note 63 at 3.
[65] *Id.* at 11.
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] Data Act, *supra* note 5, art. 4(6), at 38.

There is a distinction to be made comparing EU copyright law and overarching data protection objectives.[70] Copyright law protects "the original expression of an idea in the form of creative works"[71] meanwhile data protection seeks to protect the information, not just its expression.[72] The Data Act, however, seems to favor one over the other, that being the protection of information, and not the expression of that information through intricately designed databases and servicing systems.

The main concern surrounding intellectual property is whether any protections can be put in place that could suitably protect trade secrets.[73] Additionally, even if an agreement were made as to the confidentiality of trade secrets, there is no guidance on the enforcement or steps that may be taken to ensure compliance with the agreement.[74] The Chamber of Commerce believes that the Act should include more stringent protections of trade secrets, such as the ability to abrogate data sharing with a party if they have failed to thoroughly protect the confidentiality of trade secrets.[75]

As with third parties, the Act requires disclosure of generated data to governmental organizations when requested.[76] This data may very likely contain trade secrets and the governmental body shall only use that data "to the extent that it is strictly necessary" to comply with requests made under Article 15.[77] Article 15 lists prevention or revival after public emergencies as an example where data must be produced to governmental agencies.[78] The

[70] STREINZ, *supra* note 35, at 918 ("data protection law and intellectual property law follow ultimately different logistics.") (citing D. Liebenau, *What Intellectual Property Can learn from Informational Privacy, and Vice Versa*, 30 HJLT 285 (2016)).
[71] *Id.*
[72] *Id.*
[73] Chamber of Commerce Report, *supra* note 63, at 12.
[74] *Id. See Also* Broadbent, *supra* note 7, at 2 (arguing that any agreement made will likely be challenging to enforce).
[75] *Id.*
[76] Data Act, *supra* note 5, art. 17(1), at 49.
[77] Data Act, *supra* note 5, art. 19(3), at 51.
[78] Data Act, *supra* note 5, art. 15(1), at 48.

Chamber of Commerce argues that the standard for required disclosure is relatively low and that public interest projects that require disclosure of data may be applied to a large array of situations.[79]

Interestingly, the Chamber of Commerce also notes that there is no requirement for governmental agencies and data holders to reach an agreement on how confidential trade secrets will be protected if disclosed, leaving a question mark on how much control the government has on private intellectual property.[80] The report also lists a potentially greater cyberattack risk to the EU if governmental agencies store disclosed data on government computers.[81] Private companies are expected to invest money and research into protecting their intellectual property while government property may not be given the same care.[82]

The Act fails to establish adequate protections for trade secrets and other confidential information when establishing requirements for data sharing.[83] Furthermore, the Act offers no additional protections, but rather expressly lowers them. Preamble 112 of the Act expressly excludes *sui generis* rights from being applied to connected products.[84] The *sui generis* right protects "substantial investment" made and protects against unlawful takings or use of the content for 15 years.[85] More specifically, the right protects databases created by EU citizens from being unlawfully accessed or utilized.[86] Therefore, data generated from connected products, no matter how intricate or advanced, may be extrapolated and used in the absence of *sui generis* rights. Trade secrets that may have taken years to perfect for any given product may be easily transferred to a third party with little to no protection against its disclosure.

---

[79] Chamber of Commerce Report, *supra* note 63, at 16.
[80] *Id.*
[81] *Id.*
[82] *Id.*
[83] *Id.*
[84] Data Act, *supra* note 5, Preamble 112 at 30.
[85] Database Directive, *supra* note 28, art. 3 and art. 7, at 25.
[86] STREINZ, *supra* note 35, at 918 (citing Database Directive, art. 7).

Lack of protection for trade secrets falls perfectly within the EU's goals of creating a "single European data space."[87] The Act aims to increase the value of EU data while simultaneously limiting US presence in the data market.[88] The Act claims that trade secrets will not be required to be disclosed unless absolutely necessary to carry out the agreement between the contracting parties.[89] Meredith Broadbent of the Center for Strategic & International Studies opines that this requirement, however, will be challenging to actually enforce.[90]

Another criticism involves the lack of clarity regarding when disclosing these trade secrets will be required and how they might negatively affect companies.[91] A statement by Digital Europe and the European Business Roundtable for Industry accurately summates the biggest strength and greatest concerns of the Act,

> Capitalizing on the value of data will be crucial for Europe's competitiveness over the next decades. But as it stands, the Data Act will force European heavyweights that have invested heavily in automation and digitalization in sectors like manufacturing, green tech and health, to give away their data, leading to a new wave of de-industrialization and putting our cybersecurity at risk.[92]

In accordance with this seemingly free-for-all data transferring scheme, a red flag is raised regarding foreign shell companies located within the EU.[93] Foreign countries operating shell companies within the EU may easily request and access data from other organizations.[94] This lack of protection may allow foreign countries to access sensitive information not previously accessible

[87] Broadbent, *supra* note 7, at 2.
[88] *Id.*
[89] Data Act, *supra* note 5, art. 5(9) at 40 (stating that: "Trade secrets shall be . . . disclosed to third parties only to the extent that such disclosure is strictly necessary to fulfill the purpose agreed between the user and the third party.").
[90] Broadbent, *supra* note 7, at 3.
[91] *Id.*
[92] *Id.*
[93] Chamber of Commerce Report, *supra* note 63, at 17.
[94] *Id.*

without negotiations or agreements between the countries and may overall harm US economic interests.[95]

Concerning connected products, the Act dispossesses companies of data generated by their own products.[96] Companies have previously been able to negotiate favorable terms for each side without government intrusion, but the Act simply allows a company's respective intellectual property to be shared without any set protections.[97] The problem exists surrounding derivative data as well.[98] Derivative data is a mix of data combined from consumer data, in contrast to raw generated data.[99] The report argues that derivative data would likely contain trade secrets and the Act does not promisingly show that this kind of data will be shielded from the disclosure requirements of the Act.[100]

The Act itself fails to make distinctions based on the use of raw or derivative data and instead groups data generated by connected products into one category.[101] Lack of assurance as to trade secret and intellectual property protection will likely discourage companies from expanding their business into the EU and from investing in the EU market.[102]

US companies are not the only ones with concerns surrounding the protection of trade secrets. In early January of 2023, a large group of EU-based companies involved within the data market released a "Joint Industry Statement" relaying their concerns surrounding the Act as well

---

[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] Law Insider, *Derivative Data Definition*, Law Insider, Inc., at 1, https://www.lawinsider.com/dictionary/derivative-data#:~:text=Derivative%20Data%20means%20any%20and,and%2For%20the%20Provider%20Data.
[100] Chamber of Commerce Report, *supra* note 63, at 3.
[101] *Id.* at 19.
[102] *Id.* at 12.

as various recommendations.[103] The statement specifically calls for the prohibition of sharing data relating to "the design, the interfaces and interactions between internal components or sub-systems."[104] If this kind of data were to be shared and implemented by other companies, competition among EU businesses would be negatively affected, which is a goal the Act is specifically attempting to achieve.[105]

The Act's free-for-all concept of data sharing, requiring the rapid sharing of data without any cost to the data user, will likely lead to data holding companies remodeling their company's framework.[106] Rooted in fear of loss of trade secrets and inevitable rising of costs, businesses will be forced to restructure their data-sharing processes in order to accommodate the Act's requirements while attempting to mitigate any risks of losing valuable trade secrets.[107]

The Act's view of prioritizing data sharing in contrast to protecting trade secrets inadequately protects intellectual property rights by solely relying on the good faith of third parties and their intentions surrounding use of the shared trade secrets.[108] The Joint Industry Statement argues that the adequate protection of trade secrets is essential to "a well-functioning internal market."[109] Additionally, trade secrets must be protected to stimulate innovation, promote fairness and create trust within the economy.[110] The statement recommends more clarification surrounding data sharing requirements and to ensure the protection of trade secrets through clarification.[111]

---

[103] Information Technology Industry Council, *Joint Industry Statement: Business Community Calls for Increasing Legislative Clarity of the EU Data Act,* Jan. 17, 2023, at 1, https://www.itic.org/documents/europe/Final-JointDataActstatement17Jan2023.pdf. [Hereinafter "Joint Industry Statement"].
[104] Joint Industry Statement, *supra* note 103 at 2.
[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] *Id.* at 3.
[110] *Id.*
[111] *Id.*

B. Aggressive Cloud Switching Requirements for Providers

The Act's objective of enlarging access to reputable cloud-servicing agents also comes with its concerns.[112] Costs of switching cloud-service agents will be tasked mainly on US providers because of their large and advanced market.[113] Notably, the Act specifically requires service providers to assist their customers in transferring to competing service providers.[114] Therefore, US providers will be responsible for a majority of the cost for their consumers to switch to other servicing providers.[115] Not only do these costs negatively affect US companies, but they also affect customers, as costs would likely be imposed on both accounts that either intend to leave or stay loyal to their provider, in order to offset the costs imposed by the Act's requirements.[116]

The Chamber of Commerce report also warns of high risk of litigation and overall costs to businesses.[117] Companies that qualify as data holders under the Act will likely undergo costly litigation surrounding data sharing obligations and whether these obligations were met under FRAND terms (Fair, Reasonable, and Nondiscriminatory).[118] Although the Act establishes dispute settlement structures, FRAND terms are still vague and obscure, not to mention expensive.[119] Data holders carry the burden of proving that they meet FRAND terms, making it harder for data holders to prevail.[120] Additionally, understanding who qualifies as a "data holder" requires a deeper understanding and will also likely be the subject of litigation.[121] Lastly, the EU government will likely impose hefty fines on foreign-owned companies.[122] High fines and risk of litigation, the

[112] Chamber of Commerce Report, *supra* note 63, at 12.
[113] *Id.*
[114] Data Act, *supra* note 5, art. 23(1) at 54.
[115] Data Act Questions and Answers, *supra* note 15.
[116] Chamber of Commerce Report, *supra* note 63, at 12.
[117] *Id.* at 18.
[118] *Id.*
[119] Chamber of Commerce Report, *supra* note 63, at 19.
[120] *Id.*
[121] *Id.*
[122] *Id.*

Chamber of Commerce argues, acts as a pressure on data holders to transfer their data while also making compliance with the Act difficult due to undefined and obscure terms.[123]

The Chamber of Commerce also argues that the Act will inhibit the availability of advanced cloud services and other high-quality technology, like artificial intelligence, which will negatively affect innovation and technological advancement within the EU.[124] Source data processing services will be required to employ initiatives to obtain functional equivalence as of the new processing service provider in the context of switching cloud-servicing agents.[125] Providers will be forced to make their services comparable to those of competing providers, resulting in a sudden decrease in diverse cloud service providers available and ultimately impair innovation.[126]

Additionally, the Act seeks to expand the availability of cloud-servicing agents while simultaneously easing the process of switching between the providers, as previously mentioned.[127] Customers are given a period of 60 days to give notice to cloud-servicing agents when they desire to switch providers.[128] Providers, however, are only given 30 days to transfer data to the new provider.[129] Requiring service providers to complete the transfer within this rigid timeline is not reasonable.[130] Switching over data from provider to provider is an expensive and intricate scheme that, if rushed, may result in the loss of data and negatively impact businesses.[131]

The Joint Market Statement released by EU business notes that cloud contracts normally require long-term contracts, in contrast to the 30-day transfer requirement implemented by the

[123] *Id.*
[124] Chamber of Commerce Report, *supra* note 63, at 21.
[125] Data Act, *supra* note 5, Preamble (92) at 25.
[126] Chamber of Commerce Report, *supra* note 63, at 22.
[127] *Id.* at 3 and Data Act, *supra* note 5, art. 23(1) at 54.
[128] Data Act, *supra* note 5, art. 25(2)(d) at 55.
[129] Data Act, *supra* note 5, art. 25(2)(a) at 54.
[130] Chamber of Commerce Report, *supra* note 63, at 22.
[131] *Id.*

Act.[132] The statement categorizes this requirement as "unrealistic".[133] The Act's attempt to achieve "functional equivalence" among cloud-servicing agents will likely inhibit competition among providers because systems will likely become substantially similar to one another. Again, a lack of protection for trade secrets will result in the release of valuable information likely to be used by competing providers.[134] Overall, an identical data sharing system may ease transfers of data within the EU, but diversity among providers gives consumers the ability to weigh their options and decide which provider suits their needs best. A diverse system will likely promote competition and innovation within the EU's data market while singularity may stunt the EU's growth in the rapidly excelling technological economy.

C. Restraints on International Data Transfers

Lastly, another huge concern is the undue restriction the Data Act places on international data transfers outside of Europe.[135] The Act sets restrictions on the transfer of non-personal data internationally.[136] Therefore, cloud servicing agents operated by US companies may not be able to transfer data from the EU to the US or vice versa, which increases the cost of operating and maintaining business with the US, while also creating risks of cyber-attacks and privacy concerns.[137]

Just like accessing and utilizing data is essential for growth within the EU,[138] cross-border data transferring is essential to globalized growth in every market around the world.[139] International

---

[132] Joint Industry Statement, *supra* note 103, at 3.
[133] *Id.*
[134] *Id.* at 4-5.
[135] Chamber of Commerce Report, *supra* note 63, at 24.
[136] *Id.*
[137] *Id.*
[138] Council Press Release, *supra* note 21.
[139] W. Gregory Voss, *Cross-Border Data Flows, the GDPR, and Data Governance*, 29 WASH. INT'L L.J. 485,487 (2020)(describing cross-border data flows as a significant aspect of 21st century globalization and "the connective tissue holding the global economy together") (citing Susan Lund, *Globalization in Transition: The Future of Trade*

data transfers are critical in major international markets such as agriculture, manufacturing, and research and development.[140] With the explosion of AI, cross-border data transfers are of even greater importance given the vast amounts of data needed to operate AI systems.[141] The ability to transfer data internationally is, all in all, "integral to the modern economy, enabling communication, financial transactions, access to a vast array of services, efficient manufacturing, medical research, and so much more."[142] Intending to increase overall data utilization within the EU,[143] the Data Act seems to be a direct force against this goal with its views on cross-border data sharing.

Article 32 expressly prevents international transfers of non-personal data held within the EU if the transfer conflicts with EU or Member State law.[144] The Chamber of Commerce Report notes that the EU, therefore, is allowed to pass any law that can restrict the international transfer of non-personal data.[145] Additionally, smaller companies may not be able to easily decipher whether a transfer would conflict with EU law.[146] Exercising caution will limit the amount of pursued data transfers which will result in loss of business to providers.[147] On the other hand, businesses may be subjected to litigation if they fail to take reasonable steps to ensure transfers do not conflict with EU law.[148]

---

and Value Chains, McKinsey Global Institute, January 16, 2019 at 13, https://www.mckinsey.com/featured-insights/innovation-and-growth/globalization-in-transition-the-future-of-trade-and-value-chains).

[140] Frank Schweitzer, *The Rise of Artificial Intelligence, Big Data, and the Next Generation of International Rules Governing Cross-Border Data Flows and Digital Trade*, White & Case, March 14, 2024 at 5, https://www.whitecase.com/insight-our-thinking/rise-artificial-intelligence-big-data-next-generation-international-rules.

[141] Frank J. Schweitzer, *The Rise of Artificial Intelligence, Big Data, and the Next Generation of International Rules Governing Cross-Border Data Flows and Digital Trade – Part 1*, 1 THE GLOBAL TRADE L.J. 103 (2024), at 104.

[142] *Id.*

[143] Council Press Release, *supra* note 21.

[144] Data Act, *supra* note 5, art. 32(1) at 58.

[145] Chamber of Commerce Report, *supra* note 63, at 25.

[146] *Id.*

[147] *Id.*

[148] *Id.*

The Global Data Alliance organization echoes the same concern as the Chamber of Commerce. As smaller businesses may lack the knowledge and expertise needed to navigate increasing legislation surrounding cross-border data transferring, expectations on their ability to access important data related to healthcare, education, as well as other needs will be lost.[149]

EU businesses also hold similar concerns. Lack of clarification on what constitutes a "conflict of law" will likely hinder transfers of data in an effort to avoid litigation or fines.[150] EU companies find this restriction unfair given the differences in risks of sharing non-personal data versus personal data under the General Data Protection Regulation (GDPR), which will be discussed further in Section 4. Sharing of personal data concerns possible infringements on fundamental rights while non-personal data concerns do not.[151] The Joint Industry Statement recommends that the clients of cloud-servicing agents be able to choose when their data may be shared internationally, rather than be subject to the undue restraints placed by the Act.[152] In agreeance with the above concerns, undue restrictions on cross-border data transferring may only help the EU gain a little bit of a footing in the data market. Although, they will likely have detrimental effects on the EU's economic growth and in prime industry markets.

D. US-Specific Industry Impacts

The Brussels Effect, a concept created by Professor Anu Bradford, puts forth the argument that the EU is the greatest holder of power among the generally powerful countries in the world, such as the US.[153] Professor Bradford apportions this power to five elements – market size,

---

[149] Global Data Alliance, *CROSS-BORDER DATA POLICY INDEX*, Global Data Alliance Trust Across Borders, July 19, 2023 at 3, https://globaldataalliance.org/wp-content/uploads/2023/07/07192023gdaindex.pdf (stating that: "As governments increasingly declare data transfers to be illegal on vague or previously unknown grounds, citizens and enterprises lose confidence that they will be able to access data for their educational, health, safety or work-related needs.").
[150] Joint Industry Statement, *supra* note 103, at 4.
[151] *Id.*
[152] *Id.*
[153] ANU BRADFORD, *THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD* (2020) at 26.

regulatory capacity, stringent standards, inelastic targets, and non-divisibility.[154] All five elements must be present in regards to a particular market industry for the EU to hold power over the international market.[155]

Concerning market size, the power of the Brussels Effect is lessened where the market may not easily substitute trade exportability to third countries or to their home markets.[156] Regulatory capacity directly correlates to the EU's "ability to exert global regulatory authority."[157] A direct example of regulatory capacity can be seen in the rate of US company compliance with the GDPR. Section 4 will discuss the GDPR in depth. Statistics from 2019 found that a majority of US companies fell within a range of somewhat compliant to fully compliant with the GDPR.[158] Along with the capacity to institute regulatory authority comes the authority to impose stringent standards through regulations.[159] The regulations set by the EU must be aimed towards inelastic targets, meaning these producers or consumers within the market have no choice but to comply with the regulation in order to continue acting in the market.[160]

Lastly, the non-divisibility aspect of the Brussels Effect is triggered when a global corporation not only complies with EU regulations but conforms its entire corporation's practices to follow the EU's standards throughout its conduct with other global countries.[161] A primary example of non-divisibility from a technical standpoint is Google's re-strategization of data

[154] *Id.* at 25.
[155] *Id.* at 26.
[156] *Id.* at 27. *See also Id.* at 26 ("Large markets have a gravitational effect on producers, pulling them toward the regulatory standards prevailing in these countries.").
[157] *Id.* at 31.
[158] Ani Petrosyan, *Level of GDPR compliance among EU and U.S. firms 2019*, Statista, January 9, 2024, https://www.statista.com/statistics/1172852/gdpr-compliance-among-eu-and-us-firms/.
[159] Bradford, *supra* note 153, at 37.
[160] *Id.* at 48.
[161] *Id.* at 53.

collection within the EU by fully changing how they conduct operations globally, in order to comply with EU regulations.[162]

Notably, the US introduced a bill in the House of Representatives called the DATA Act (Deterring America's Technological Adversaries Act) on February 24, 2023.[163] Unlike the EU's Data Act, the US DATA Act is tailored towards imposing punishments against persons who unlawfully transfer "sensitive personal data" to the People's Republic of China and aims to better protect US national security.[164] Although these two Acts aim to achieve very different goals, it is, nevertheless, an example of the influence the EU regulation has on its powerful country counterparts.

This section will argue that, because the US heavily relies on the EU's data in crucial sectors of our economy, any restrictions on the US' access to this data may have a crippling negative effect on US industries generally, as well as innovation within those industries. US reliance on the EU concerning specific market industries may trigger the Brussels Effect, putting the US under the power of the EU in those specific markets.

The Chamber of Commerce Report identifies several industries within the US that will likely be negatively impacted by the Data Act.[165] The automobile industry in the US relies heavily on EU-manufactured vehicles.[166] This, in turn, triggers the Brussels Effect, as the US most likely cannot easily transport their automobile market to third countries or to their home market corporations.[167] Along with automobile manufacturing comes data generation and any restricted

[162] *Id.* at 57. (citing Ryan Singel, EU Tells Search Engines to Stop Creating Tracking Databases, WIRED April 8, 2008, http://www.wired.com/threatlevel/2008/04/eu-tells-search/).
[163] Deterring America's Technological Adversaries Act, H.R. 1153, 118th Cong. (2023).
[164] *Id.* at 2.
[165] Chamber of Commerce Report, *supra* note 63, at 26.
[166] *Id.*
[167] Bradford, *supra* note 153, at 27.

access to data generated by vehicles made in the EU will most likely negatively impact the US automobile industry, as well as the global automobile industry.[168]

Specifically, vehicles are built by Original Equipment Manufacturers (OEMs), which specifically rely on data in order to enhance the safety of the car.[169] OEMs require access to vast amounts of vehicle safety data in order to accurately decipher the best course of action for a car's safety manufacturing features.[170] Restricted access to this data for OEMs may have a significant negative impact on the industry at large.[171]

Air travel is another industry likely to be negatively impacted by the Data Act.[172] OEMs utilize Aircraft Condition Monitoring Systems (ACMS) which store operational data, which is then given to operators of the aircraft.[173] Operational data is used to understand how the engine and other aircraft systems operate.[174] This data is considered to be intellectual property due to the labor-intensive research undertaken to collect the data and then develop services and solutions based on the data.[175] When aircraft operators negotiate contract terms regarding data sharing, they agree on steps taken to ensure protection of the data and other confidential information that may be shared.[176] The Act poses a threat to the rigid negotiation structure already set in place between aircraft operators and other data holders within the aviation industry.[177] The Act's flawed protection system set for trade secrets and other intellectual property may lead to a decreased

[168] Chamber of Commerce Report, *supra* note 63, at 26.
[169] *Id.*
[170] *Id.*
[171] *Id.*
[172] *Id.* at 27.
[173] *Id.*
[174] *Id.*
[175] *Id.*
[176] *Id.*
[177] *Id.*

amount of data collection in order to avoid data transferring and sharing, which will lead to a stunt in development within the industry.[178]

The EU data market is dominated by US technology companies.[179] The Act serves to help give EU companies a leg up on US companies to help shift the market power in favor of EU companies and reduce any dependency on US cloud servicing providers.[180] More specifically, the Act seemingly seeks to decrease US competition with EU companies by making it easier for EU companies to take customers from US companies. A proposed EU Cloud Certification Scheme (EUCS) would make it difficult for US companies to receive security certifications solely because of their headquartered location, making it easier for customers to switch over from reputable US cloud servicing providers to EU providers.[181]

The pharmaceutical and medical device industry in the EU relies heavily on trading with the US.[182] As expected, the industry holds its fair share of trade secrets and valued intellectual property which requires years of research and data collection to obtain and understand.[183] The Data Act particularly places the industry in a weaker position because of its lack of protections placed on trade secrets and intellectual property and also because the industry relies on data sharing and transferring in order to continue innovating and improving healthcare in our society.[184] Any restrictions that may be placed on the US' ability to obtain data from the EU will inhibit the research and development of significant medical devices and pharmaceuticals.[185] Without access

[178] *Id.*
[179] *Id.* at 28.
[180] *Id.*
[181] Kenneth Propp, European Cybersecurity Regulation Takes a Sovereign Turn, Atlantic Council, September 13, 2022, https:// www.crossborderdataforum.org/european- cybersecurity-regulation-takes-a-sovereign- turn/.
[182] Chamber of Commerce Report, *supra* note 63, at 29.
[183] *Id.*
[184] *Id.*
[185] *Id.*

to this data, healthcare organizations may be compelled to undergo research and development in third countries, likely incurring high relocation costs and loss of capital placed in the EU.[186]

Financial institutions regularly negotiate contracts regarding data sharing.[187] The Data Act seems to place limitations on contractual capabilities which may make it harder for companies to not only negotiate with each other but also come to terms on important issues within the industry.[188] Additionally, US institutions place heavy reliance on data sharing with EU institutions, which will likely be negatively impacted by any restrictions placed on non-personal data transferring and sharing.[189] This is particularly important because data transferring for financial institutions is crucial for continuing to provide financial services and support the economy.[190]

E. Recommendations

Key weaknesses of the Data Act include the Act's relatively weak protections surrounding trade secrets and confidential information, as well as the negative impacts prime US industries will face because of the restricted regulation on cross-border data sharing. Although the Act seeks to achieve greater circulation and utilization of data throughout the EU, another primary goal is to establish a singular data market that prioritizes EU organizations and data holders.[191] With the US-based companies being primary data holders with bases in the EU, these companies are at both a financial and legal risk.

Financially, these companies will likely be put at a disadvantage with respect to EU companies concerning data sharing, which will hinder innovation and development.[192] Legally, US companies face a high litigation risk due to vague data sharing rights surrounding international

[186] *Id.*
[187] Chamber of Commerce Report, *supra* note 63, at 30.
[188] *Id.*
[189] *Id.*
[190] *Id.*
[191] Impact Assessment Report, *supra* note 30, at 33.
[192] Chamber of Commerce Report, *supra* note 63, at 11.

company's data sharing with the EU. The high risk of litigation along with its high costs will most likely deter many US companies from sharing data with the EU.[193]

Ultimately, there is an argument to be made that the Act may keep the EU at a standstill in regard to data utilization and sharing. With the US facing strong barriers and deterrents against data sharing with the EU, vast amounts of valuable data will likely go unstudied, which was the overall problem the Act was trying to solve.[194] The Act might help EU companies gain better control over the data market, however, requirements for service providers to shape their services comparable to other service providers to make switching providers easier; will likely result in less competition because of the lack of variety of different services being offered to consumers.[195]

Many changes should be made to the Act to more efficiently reach the EU's data market goals while also protecting the rights and values of other countries and consumers. In an effort to achieve a singular data market within the EU, clarifications must be made surrounding the specific data-sharing requirements outlined in the Act's provisions in order to better assist EU companies in following their respective duties. Greater clarification will give companies a better sense of what kind of data falls under the Act, when it must be shared, and whom it must be shared with. Greater protections must be implemented to protect company trade secrets in order to protect valuable assets of a company, maintain diverse standards within the market, and promote competition among service providers.[196] Lesser restrictions surrounding international data transferring will also likely result in a greater sharing and use of valuable data within the EU.

IV. Interplay with the GDPR

[193] *Id.* at 18.
[194] Council Press Release, *supra* note 21.
[195] Data Act, *supra* note 5, Preamble (92), at 25.
[196] Chamber of Commerce Report, *supra* note 63, at 12.

The European Council passed the GDPR in 2016 as a massive step forward in protecting personal data generated within the EU.[197] Generally, anyone who utilizes personal data generated from citizens of the EU must comply with the GDPR.[198] One of the main goals of the GDPR is to give individuals access to the data they personally generate.[199] Along with easier access, the GDPR aims to help individuals explain how their data is being used while making it comprehensible.[200] The regulation also opens doors to allow for personal data transfer between providers, establishes a right for data to be forgotten, and further protects consumers by requiring companies to notify when data breaches have happened.[201] Overall, the GDPR focuses mainly on the transfer of personal data within or outside of the EU.[202]

Concerns have arisen regarding the interoperability of the Data Act with the GDPR.[203] The GDPR, covering mainly personal data, has now been followed by the Data Act, which governs both personal and non-personal data. Notably, the Data Act operates without prejudice to the GDPR.[204]

One concern regarding the Data Act's operability in conjunction with the GDPR is how data holders will be able to make distinctions concerning personal and non-personal data when trying to comply with both the Data Act and data privacy laws concerning personal data, like the

---

[197] Council Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. L 119 [hereinafter GDPR].
[198] Ben Wolford, *What is GDPR, the EU's new data protection law*, GDPR.eu, https://gdpr.eu/what-is-gdpr/.
[199] Publications Office of the European Union, *Summary of: Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data*, EUR-Lex, Jan. 7, 2022, at 1, https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html - :~:text=The GDPR offers various instruments, codes of conduct and certification.
[200] *Id.*
[201] *Id.*
[202] Barbara Da Rosa Lazarotto, *The Data Act: a (slippery) third way beyond personal/non-personal data dualism?*, European Law Blog, May 4, 2023, https://europeanlawblog.eu/wp-content/uploads/2023/05/Blogpost-202023.pdf [hereinafter "European Law Blog"].
[203] Chamber of Commerce Report, *supra* note 63, at 20.
[204] Data Act, *supra* note 5, art. 1(5), at 33.

GDPR. The US Chamber of Commerce questions how data holders will be able to comply with the transfer of data to other parties and be able to decipher whether the data being transferred is personal to comply with personal data privacy rights.[205] The report emphasized that personal data is encrypted and anonymous and should remain inaccessible to outside parties.[206] When factoring in family devices that generate collective data, understanding how to and when to share this data is a gray area and will likely be subject to litigation.[207]

Additionally, ambiguities as to terms written in both regulations give rise to confusion.[208] Both regulations set standards that must be met when seeking to transfer data outside of the EU.[209] For example, the GDPR allows the transfer of data to third countries if the country is found to have "adequate protections" in place.[210] In contrast, the Data Act requires the third country and the EU or Member State to have an international agreement or, if there is no agreement, a governing body that can adequately decipher if the data to be transferred is proportionate to its request.[211] These different requirements raise questions as to what a data holder must follow. The risk of substantial fines and costly litigation would likely deter providers and data holders from transferring data to third countries.[212]

Lastly, the lack of clarity surrounding the Act's broad definition of data poses concerns surrounding potential conflicts with the GDPR. EU companies believe the Act's definition of data is "unclear, too broad and general."[213] An unclear and overbroad definition of data will result in companies storing and processing excess data that may not be needed in order to ensure

[205] Chamber of Commerce Report, *supra* note 63, at 20.
[206] *Id.*
[207] *Id.*
[208] European Law Blog, *supra* note 202.
[209] *Id.*
[210] GDPR, *supra* note 197, art. 45(1), at 61.
[211] Data Act, *supra* note 5, art. 27, at 56.
[212] European Law Blog, *supra* note 202.
[213] Joint Industry Statement, *supra* note 103, at 2.

compliance with the Act's data-sharing provisions.[214] The storage and use of unnecessary data might cause conflict with the GDPR's goal of data minimization.[215] Specifically, one of the critiques of the GDPR surrounds its failure to address potential changes that might develop within the data economy and the overall goal to maximize "the economic and social value of personal data."[216] Following any potentially unnecessary utilization of data, a risk of conflict may arise with the Data Act's requirements to share data and with the GDPR's data protection rights surrounding personal data and goals of data minimization.[217]

V. Conclusion

Although the Data Act was proposed with hopes of making big advancements in EU data sharing, the Act's application falls short in different ways. First, the Act unduly restricts cross-border sharing with international countries, like the US. Lesser restrictions surrounding international data transferring will likely result in greater sharing and use of valuable data within the EU, which is a main goal for the EU. Another failure of the Act is the lack of trade secret and intellectual property protection. Trade secrets that may have taken years to perfect for any given product may be easily transferred to a third party with little to no protections against its disclosure. Greater protections must be formulated to protect company trade secrets in order to protect the valuable assets of a company, maintain diverse standards within the market, and promote competition among service providers.

Lastly, clarifications should be made regarding any overlap between the application of GDPR and the Data Act's provisions. Greater clarification will give companies a better sense of

---

[214] *Id.*
[215] *Id.*
[216] STREINZ, *THE EVOLUTION OF EUROPEAN DATA LAW*, *supra* note 35, at 910 (citing T Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L REV 995 (2017).
[217] *Id.* at 909.

what kind of data falls under the Act, when it must be shared, and whom it must be shared with. Different requirements raise questions as to what a data holder must follow which will either force companies to undergo a risk of paying fines or endure costly litigation. The risks associated with potentially violating the Act may ultimately disincentivize companies from heavily competing within the EU data market. In order to better achieve a singular data market and increase access to valuable data within the EU, greater clarification surrounding the Act's provisions, stricter trade secret protections, and lesser restrictions on international data transfers are of top priority among recommendations for a better and more unified EU.