Feedback on the Data Act

The Center for Data Innovation (Transparency Register #: 367682319221-26) is pleased to submit this feedback on the European Commission's proposal on harmonised rules on fair access to and use of data (Data Act).[1]

THE DATA ACT IS COMMENDABLE BUT NEEDS ADJUSTMENTS

Responsible data sharing is not only critical to the digital economy but also to the whole European economy. The European data economy has grown at a year-over-year rate and now accounts for 3.6 percent of European Union (EU) GDP and was valued at over €440 billion in 2021.[2] By 2030, the EU data economy should cross the €1 trillion threshold.[3]

Adopted on February 23, 2022, the Data Act follows the Data Governance Act as part of the European Commission's greater European data strategy.[4] The Data Act addresses who can access and innovate using data generated by Internet of Things (IoT) connected devices, cloud services, and edge services. Specifically, the Act clarifies how economic sectors, public sector bodies, IoT manufacturers, suppliers of related services, data holders, data recipients, and other businesses can access and share data generated from consumer use of Internet-connected devices to benefit two stated beneficiaries—European small and medium-sized enterprises (SMEs) and consumers.[5]

Unfortunately, the Data Act contains fundamental pitfalls and needs significant modification to not harm the European data economy. Among other concerns, the Act could increase barriers to entry for

[1] European Commission, "Data Act: Proposal for a Regulation on harmonised rules on fair access to and use of data" (Brussels: European Commission, February 23, 2022), https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data.
[2] Lisbon Council and IDC for the European Commission, "European Data Market Study 2021–2023 D2.1 First Report on Facts and Figures. Version 1.2" (Luxembourg/Gasperich: European Commission, January 31, 2022), https://digital-strategy.ec.europa.eu/en/library/results-new-european-data-market-study-2021-2023.
[3] Lisbon Council and IDC, "European Data Market Study 2021–2023."
[4] European Commission, "Data Act | Shaping Europe's digital future," March 16, 2022, https://digital-strategy.ec.europa.eu/en/policies/data-act.
[5] European Commission, "Commission Staff Working Document. Impact Assessment Report. Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)" (Brussels: European Commission, February 23, 2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022SC0034&qid=1647476394617.

businesses, treat international cross-border data flows unfairly, raise privacy concerns regarding government use of data, and muddle the interactions with other EU data-focused legislation.

To carefully balance competition, innovation, and privacy in the EU, the European Commission should start by revising the Data Act to:

1. Minimize the burdens of compliance and barriers to entry for all IoT companies, domestic and foreign, seeking to provide their services to European consumers. (i.e., Recital 19, Article 30, etc.)
2. Clarify the Act's effect on international data flows to make the EU data economy more competitive, not less, to multinational companies and global innovators. (i.e., Explanatory Memo's Subsidiarity, Article 27, etc.)
3. Balance privacy safeguards with data accessibility in business-to-government sharing to protect against misuse of consumer data from connected devices. (i.e., Chapter Five, Article 17, etc.)
4. Mitigate legislative fragmentation that could result from the Act's interactions with the Digital Markets Act and the General Data Protection Regulation (GDPR). (i.e., Article Five, Article Six, etc.)

KEY STRENGTHS OF THE DATA ACT

The Data Act aims to ensure that data-driven and innovative solutions can thrive in the EU by making data from connected devices more easily accessible in the internal market. The following explains some of the ways the Act makes it easier for companies and consumers to harness the data users generate.

CREATES A CLEAR FRAMEWORK FOR THE INTERNAL MARKET

The Act clarifies the current patchwork of EU rules on non-personal data. As described by the Commission itself, further legislative fragmentation between member states on the treatment of data can lead to "higher transactional costs, lack of transparency, legal uncertainty and undesirable forum shopping," [6] By addressing these issues and ensuring that businesses have one consistent framework to follow, the Act will clarify data flows in the internal market—something IoT services can use to provide more innovative products and devices to Europeans. The Data Act will also rectify post-GDPR legislative fragmentation caused by member states by standardising data sharing and accessibility requirements supranationally.[7]

[6] European Commission, "Data Act," Explanatory Memo.
[7] "Data Protection Laws of the World," DLA Piper, 2021, https://www.dlapiperdataprotection.com/?t=law&c=DE.

Companies currently rely on both personal and non-personal data to fine-tune their services internationally. The Data Act establishes cross-border data flows within the EU to ensure that businesses are not confused or burdened by having to navigate a patchwork of regulations. This will also ensure companies do not over-concentrate into a single member state to avoid over-regulation by another national legislature. Both effects could make it easier for services to provide European consumers with more innovative, more accessible IoT services.

FOSTERS GOVERNMENT USE OF DATA FOR THE PUBLIC GOOD

The Act ensures that European member states and businesses consider the benefits of public use of data, which could be especially useful in sectors and for emergencies where data-sharing will have the most benefit. The explanatory memo highlights a clear understanding that legal uncertainty and commercial disincentives impeded the potential public sector use of data in emergencies and crisis management scenarios.[8] This is further supported by how Chapter Five in the Act delineates obligations for both businesses and public sector bodies on how to make data generated by users available and treat the received data.[9]

The Data Act clearly acknowledges how business-to-government data sharing can be useful in the internal market. Business-to-government data sharing can be especially timely for emergencies like military conflicts or pandemics, where ways to use mobility and location data on connected devices can support public health and humanitarian strategies.[10]

OPPORTUNITIES TO IMPROVE AND RECOMMENDATIONS

The following explains some of the main issues with the proposed legislation and provides recommendations on how to alleviate these concerns.

INCREASES BARRIERS TO ENTRY INTO THE EUROPEAN DATA MARKET FOR BUSINESSES

The Data Act imposes certain obligations on businesses to collect and share IoT data that increase the barriers to entry for Europe's start-ups and SMEs. In Recital 19, the Act even specifies its intention for all data-driven products to be "designed and manufactured and related services are provided in such a manner that data generated by their use are always easily accessible to the

[8] European Commission, "Data Act," Explanatory Memo.
[9] European Commission, "Data Act," Chapter V.
[10] Hodan Omaar, "How the EU Can Unlock the Private Sector's Human-Mobility Data For Social Good" (Center for Data Innovation, March 2022), https://s3.amazonaws.com/www2.datainnovation.org/2022-mobility-data-social-good.pdf.

user."[11] Article Three's "obligation to make data generated by connected devices accessible" also begins at the design phase of a product.[12]

In specific contexts like Article 30, which establishes requirements regarding smart contracts for data sharing, the Data Act is likely to entrench established businesses that already have the capacity to handle higher costs as well as legal and technical requirements at the onset. The Act attempts to solve this issue in Articles Seven and Article 16 of the Data Act, where it exempts SMEs from the Data Act's Chapters Two and Five as defined by Article Two of a different piece of legislation, the Enterprise Size and Commission Recommendation:

> ...a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed €10 million. A microenterprise, which also falls under the SME category, is defined as an enterprise which employs fewer than ten persons and whose annual turnover and/or annual balance sheet total does not exceed €2 million.[13]

This explicit carveout to protect European SMEs is misguided, as rules should apply to all businesses irrespective of their size. Moreover, this attempt to protect European SMEs will fail as all businesses will still have to follow the ethos of the legislation.[14] Both chapters create standards for data sharing in the EU. Chapter Two establishes guidelines for business-to-consumer and business-to-business data sharing, and Chapter Five establishes guidelines for business-to-government data sharing.[15] Because size-based distinctions can be arbitrary and fail to account for businesses' growth trajectories, business plans, and even potential losses, businesses of all sizes—regardless of if they are currently exempted from Chapters Two and Five—will focus on complying with the entirety of the Data Act.

Companies that desire to scale up in the future will be pushed to dedicate staff to compliance, increase their expenses, and more to comply with those data sharing standards. All companies will be compelled from product conception and design to consider how easily accessible their data is upon consumer request, even if it comes at the expense of product quality. In fact, Articles Three and

[11] European Commission, "Data Act," Recital 19.
[12] European Commission, "Data Act," Article 3.
[13] European Commission, "Enterprise size and Commission Recommendation," August 9, 2017, https://www.ecb.europa.eu/stats/money_credit_banking/anacredit/questions/html/ecb.anaq.170809.0001.en.html.
[14] European Commission, "Data Act," Chapter II. European Commission, "Data Act," Chapter V.
[15] European Commission, "Data Act," Chapter II. European Commission, "Data Act," Chapter V.

30 could be interpreted as pushing companies currently on the market to reengineer entire portions of how their products and services function to ensure future compliance.

The complexity of the EU's digital regulations is already a critical roadblock to innovation for EU SMEs in the data economy.[16] In one survey of EU data companies, only 34 percent of the SMEs even had data-sharing in their strategy.[17] Another survey highlighted how European SMEs would redirect resources towards compliance when faced with restrictions on data flows and data sharing, regardless of their smaller size in comparison with very large online providers.[18]

The Data Act will have similar results as its regulatory burdens will make it harder for European companies to compete internationally. Europe will be tying its start-ups and businesses in an environment that is not nearly as light-touch as other global data economies. International competitors from other high-tech markets, like India, the United Kingdom, and even the United States, will be less burdened with compliance in their own data markets and will thus be able to invest more in research and development. European companies looking to enter those markets will be less competitive and potentially less innovative because they will have to face the budgetary constraints of EU legislative compliance beforehand.

Recommendation:

To mitigate these issues, the Commission should modify the Articles within Chapters Two and Five regarding business-to-business and business-to-government data sharing to remove or at least alleviate some of the regulatory hurdles businesses may face when entering or operating in the European data market. Caveats like Articles Seven and 16 that exempt SMEs are carve-outs that cannot be long-term solutions and will not make innovative EU start-ups competitive globally. These businesses will still have to comply with other Chapters of the Act, will still face higher compliance costs, and will still look to comply with the exempted chapters to scale up in the future. Rather than attempt to exempt SMEs from onerous regulations, which distorts the market and leads to a larger share of less productive SMEs, the Commission should seek to both lower the compliance burden for all businesses and remove any carve-outs that treat businesses differently based on arbitrary size distinctions.

---

[16] Katri Korhonen, "European companies struggle to get aboard the data economy," SITRA, May 23, 2021, https://www.sitra.fi/en/articles/european-companies-struggle-to-get-aboard-the-data-economy/.
[17] Katri Korhonen, "European companies struggle to get aboard the data economy."
[18] Frontier Economics, "Beyond Personal Data: Cost of Data Flow Restrictions to EU Companies" (February 2022), https://www.frontier-economics.com/media/5065/beyond-personal-data_the-cost-of-data-flow-restrictions-to-eu-companies.pdf.

The Committee should adjust how the Act treats data collection to ensure Europeans have the most innovative products in the market. Rather than pushing businesses in Recital 19 and Article Three to consider data collection at the design phase, the Commission should tailor the proposal to ensure that if IoT businesses collect and store data generated by their consumers, they have taken the appropriate measures to ensure that if requested the data can be portable and accessible without undue delay. Suppose businesses do not collect and store data because of capacity constraints. In that case, the Commission should ensure each business has the time needed to innovate while actively taking measures to grow their capacity to collect the desired data in the aftermarket. Further, while the Commission explicitly states the Act should not affect trade secrets or intellectual property rights, it should ensure so by eliminating Articles 4(3), 5(8), and 19 (2)—three sections of the Data Act that push for businesses to disclose trade secrets after enacting measures to preserve their confidentiality. These are provisions that harm incentives to share data and could steer businesses away from launching or providing Internet-connected devices and related services in the EU data economy.

With these adjustments, the European market would be more competitive for launching start-ups and providing users with new, innovative services.

UNFAIR TREATMENT OF INTERNATIONAL CROSS-BORDER DATA FLOWS

In the explanatory memo, the Commission clearly understands how vital a unified legal regime is to the data economy. The Commission writes, "many private actors who hold relevant data are multinational companies. These companies should not be confronted with a fragmented legal regime."[19] This concern over legislative fragmentation continues throughout much of the proposal, ensuring that overly burdensome digital regulation will not interfere with cross-border data flows in the internal market.[20]

Unfortunately, the EU's understanding of the importance of cross-border data flows ends at its own borders. Cross-border data flows have historically been used to track supply chains, push technological innovation, and drive international economic relationships, and this value has only grown in the data economy.[21] Nevertheless, while the Commission worries about barriers to entry for data sharing within the EU, the proposed Act will stifle global data sharing. Chapter Seven in the Act describes how international transfers of "non-personal data held in the Union" by data processing

[19] European Commission, "Data Act," Explanatory Memo.
[20] European Commission, "Data Act," Explanatory Memo.
[21] Kristin Archick and Rachel F. Fefer, "US-EU Privacy Shield and Transatlantic Flows" (Congressional Research Service, September 2021), https://crsreports.congress.gov/product/pdf/R/R46917.

services will be restricted if the transfer could create a conflict with Union Law or if there was no existing international agreement or tribunal decision.[22]
In practice, if the Data Act is more burdensome than other global regulatory structures, it could create legislative fragmentation that will slow international data flows for non-personal data, which could lead other nations to impose reciprocal restrictions on affiliates of EU companies in other nations. When surveyed, 40 percent of EU companies considered "regulations which require them to assess the laws and practices of non-EU countries they share non-personal commercially sensitive with" as effectively requiring them to stop those cross-border data flows.[23]

Multinational companies would find it harder to access European data from their connected devices or even from European IoT companies—disrupting how global companies innovate and collaborate by reducing their research and development capacities, increasing the cost of products, and reducing the quality of services.[24] Worse, this could make it harder for the EU to entice multinational companies to enter the EU data market as it would hand burdensome restrictions to non-EU companies choosing to operate in the market. The Act's restrictions on international data flows could also significantly make it harder for EU companies to rely on international data sharing to remain competitive or economically scale up. Moreover, there is no legitimate public interest rationale for restricting the movement on non-personal data outside of the EU.

Recommendation:

The Commission needs to compare the Data Act to other data sharing regulations globally before deciding how to address regulating IoT data at the Union level. The Data Act currently restricts international data transfers too severely compared to other competitive international regulations and could strangle Europe's access to international companies, international data, and international innovation.

Instead, the Commission should translate how it wants the free flow of cross-border data sharing in the internal market to how it will treat the international data economy and focus on making the Data Act competitive legislatively. To ensure the European data economy is a market that companies want to enter, the Commission should eliminate some of the provisions mentioned below from the business-to-business data sharing provisions in Chapter Two and the international access and

[22] European Commission, "Data Act," Chapter VII. European Commission, "Data Act," Article 27.
[23] Frontier Economics, "Beyond Personal Data: Cost of Data Flow Restrictions to EU Companies."
[24] Marjorie Chorlins, "U.S. Chamber Statement on the European Commission's Proposal for a New Data Act," February 23, 2022, https://www.uschamber.com/international/u-s-chamber-statement-on-the-european-commissions-proposal-for-a-new-data-act.

transfer requirements of Chapter Seven and Article 27.[25] In Chapter Two, for example, the Commission could look to remove the aforementioned presumption of data collection at the design phase in Article Three, or the discussion of disclosing trade secrets to third parties in Article Five.[26] In Chapter Seven and Article 27, another example of a potential provision to eliminate or modify is the use of the European Data Innovation Board to create and develop further guidelines to assess international data transfers.[27]

PRIVACY CONCERNS OVER THE GOVERNMENT'S USE OF DATA

In Chapter Five, the Act discusses how companies must make data available to the public sector and government institutions in cases of "exceptional need," but it does not clearly define the scope of exceptional need or the government's discretion in creating such an obligation.[28] Article 15 attempts to qualify the "exceptional need to use data" as applicable when in response to, to prevent, or to assist in the recovery from a public emergency or when a specific task done in the public interest does not have or cannot obtain by alternative means the needed data.[29]

Unfortunately, this section does not limit what type of data is to be shared, how long it is to be shared, or how it will be safeguarded. The nature of the request, while delineated in Article 17, does not specify ways to safeguard the public from institutional misuse or from bad actors who could use business-to-government data sharing as an opportunity to exploit weakened data security. Article 17 clarifies what a public institution should list when requesting data, including what data, the exceptional need, and the purpose of the request while Article 19 defines the obligations a public sector body has to safeguard the privacy of any subjects' personal data and destroy it when finished.[30]

But neither Article 17 nor Article 19 limits how long a public institution can have access to the data, what the safeguards must entail, or the limits on how granular they can request the data. By not having these specifications designed to protect the European public, the discretion provided to these institutions and bodies could be ripe for generous interpretation and, in the worst of cases, abuse. The Commission does attempt to protect personal identifiable information in Article 18(5) by pushing

[25] European Commission, "Data Act," Chapter II. European Commission, "Data Act," Chapter VII. European Commission, "Data Act," Article 27.
[26] European Commission, "Data Act," Chapter II.
[27] European Commission, "Data Act," Article 27.
[28] European Commission, "Data Act," Chapter V.
[29] European Commission, "Data Act," Article 15.
[30] European Commission, "Data Act," Article 17. European Commission, "Data Act," Article 19.

data holders to reasonably pseudonymize all data, but does not specify what the Commission considers legally effective pseudonymization of personal and non-personal data.

Recommendation:

To ensure that Europeans' privacy is top of mind, the Commission should provide sufficient clarification and privacy safeguards within this chapter. Providing further clarification on what qualifies as a public emergency or exceptional situation and the requirements on how the government can treat the data obtained would be a good start.

The Commission should amend Articles 17 and 19 to further clarify the limits public institutions will have to prevent misuse and safeguard Europeans' privacy. This should include but not be limited to clarifying the maximum length of time institutions can hold data, what security measures should be in place, and what exactly an organization needs to provide in order to determine if there is an exceptional need for the requested data. By limiting the potential for misuse, the Commission can ensure any business-to-government data sharing remains safe, secure, and with privacy as a priority.

UNCLEAR INTERACTIONS WITH OTHER EU DATA-FOCUSED LEGISLATION

Despite sections of both the explanatory memorandum and legislative text ensuring that the Act works in conjunction and parallel to current European digital legislation, the Data Act is still unclear on which legislation will take precedence over one another in unclear situations. The legislative proposal focuses on data from connected devices writ large, with sometimes no real distinction between personal and non-personal data on the services in question. But the lack of clarity between personal and non-personal data brings the interplay with the GDPR into question with regard to every reference to unspecified data. It will be crucial to clarify this interaction to mitigate any supranational legislative fragmentation before being taken out of policymakers' hands.

Articles Five and Six, in particular, target what the Digital Markets Act deems as gatekeepers — a term used to describe the largest online service providers globally—to limit how, even upon request of a user, these companies receive the benefits of data sharing as delineated in the Data Act.[31] Article Five states that data holders should make data generated by their use available to third parties when users or parties acting for users ask.[32] Yet Article Five also excludes gatekeepers as eligible third parties for receiving shared data.[33] Article Six further explains that other third parties

[31] European Commission, "Data Act," Articles 5. European Commission, "Data Act," Article 6.
[32] European Commission, "Data Act," Article 5(1).
[33] European Commission, "Data Act," Article 5(2).

cannot then make the Data-Act enabled data sharing available to Digital Markets Act-deemed gatekeepers.[34] This is a discriminatory provision that will not boost data innovation.

Recital 36 further explains this interaction as not preventing "these companies from obtaining data through other lawful means."[35] However, even this narrowed scope could potentially interact and overlap with the GDPR right to data portability.[36] While the Data Act focuses on European consumers' ability to ask for their non-personal data to be portable, Article 20 in the GDPR ensures that European consumers of online services have the right to receive and port their personal data.[37]

The GDPR does not differentiate based on the size of a company when it comes to a user or data subject's right to portability. So, which should supersede the other, the GDPR right to data portability for personal data or the Data Act ban on data portability to gatekeepers of unspecified data?

The proposed Act attempts to explain and rectify this with the following section of Recital 36:

> "The [Regulation on contestable and fair markets in the digital sector (Digital Markets Act)] aims to redress these inefficiencies and imbalances by allowing the Commission to designate a provider as a "gatekeeper", and imposes a number of obligations on such designated gatekeepers, including a prohibition to combine certain data without consent, and an obligation to ensure effective rights to data portability under Article 20 of Regulation (EU) 2016/679."[38]

Unfortunately, even this clarification lends itself to more regulatory questions than answers. It highlights an imbalance between the GDPR's right to portability for all users versus the Data Act's exclusion of Digital Markets Act-qualified gatekeepers. While the Digital Markets Act may be GDPR-compliant, that does not necessarily mean applying the Data Act restrictions defined in Articles Five and Six will be, especially considering how the spectrum of what constitutes Data Act data-sharing and GDPR data portability will overlap in practice.

[34] European Commission, "Data Act," Article 6.
[35] European Commission, "Data Act," Recital 36.
[36] European Commission, "General Data Protection Regulation (GDPR)" (Brussels: European Commission, May 23, 2018), Article 20, https://gdpr-info.eu/art-20-gdpr. European Commission, "GDPR," Recital 68.
[37] European Commission, "GDPR," Article 20.
[38] European Commission, "Data Act," Recital 36.

Recommendation:

The interaction with the Digital Markets Act and GDPR is just one example of the lack of clarity in how the Data Act interacts with multiple pieces of EU digital legislation.[39]

The Commission should clarify which data it refers to consistently throughout the proposal. The Commission should also clarify how the interactions with the Digital Markets Act and GDPR would work in the proposal to mitigate this potential legislative grey area. The Commission's second step should be to more clearly delineate the Data Act's relationship with many of the EU data-driven innovation proposals on the table—including but not limited to the new cross-border data flow agreement with the United States.[40]

CONCLUSION

As it stands, this legislative proposal threatens to burden entrepreneurs and online services with over-regulation in an attempt to help EU small businesses and the European digital economy. While its underlying goal—data-driven innovation bolstered by data from connected devices and the IoT—is commendable, the Data Act fails to understand the complex nature of data governance, data protection, and data competition. By focusing solely on the internal market with regards to cross-border flows and data accessibility, the Data Act has laid the foundation for a European data economy that will be less innovative internationally, more susceptible to private and public bad actors, and less able to get IoT start-ups off the ground.

The Commission should further refine the Data Act to help promote innovation in Europe's data economy. When an industry study defines the cost of potential data restrictions as about €80 billion per year, the European Commission needs to closely look at the unintended consequences of the Data Act and its aforementioned provisions to ensure that the impact benefits both European consumers and European SMEs.[41]

If the European Commission starts with narrow adjustments in the Data Act's scope, it can ensure companies treat the European market as a more friendly market internationally for data-driven innovation, and users are more likely to have faith in their privacy in the IoT.

---

[39] Inge Graef and Martin Husovec, "Seven Things to Improve in the Data Act," March 7, 2022, https://ssrn.com/abstract=4051793.

[40] The White House Briefing Room, "FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework," March 25, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.

[41] Frontier Economics, "Beyond Personal Data: Cost of Data Flow Restrictions to EU Companies."