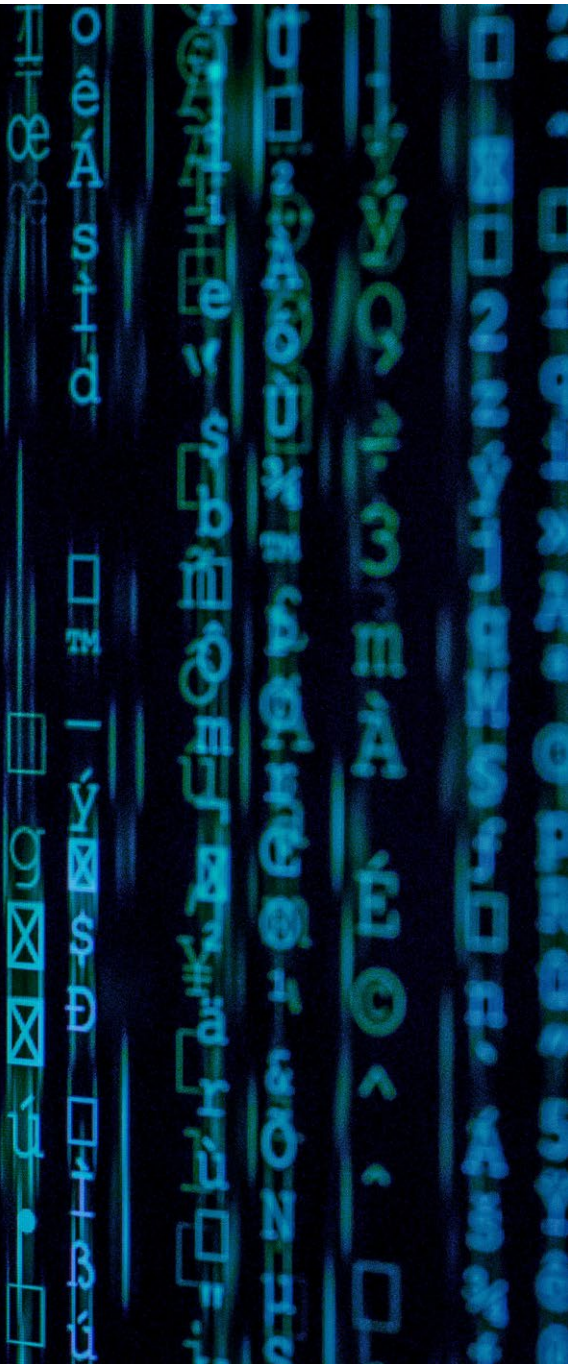
POLICY BRIEF: DATA TRUST

By Kimberly A. Houser
Center for the Governance of Change
April 2024

EXECUTIVE SUMMARY



How can firms unlock the potential of data to increase innovation and promote social good, while at the same time protecting data subjects? While the EU is ahead of other regions in terms of considering and addressing potential data harms, EU's legal regime around data use has two main shortcomings. First, it is not flexible enough to address emerging technologies and data uses, and second, the regulatory lag means that by the time a regulation comes into force, it may be out of date.

What is needed is a flexible customizable device subject to appropriate guardrails that can hold and determine data use in line with the rights and values of data subjects. According to the OECD, SMEs "are fundamental to innovation, economic growth and job creation, and play a critical role in social cohesion,"[1] yet their growth in the EU is stymied by strict data protection laws. Additionally, these potential innovators lack access to the troves of data held by Big Tech, nor is privately collected data easily accessible for research purposes or social good.

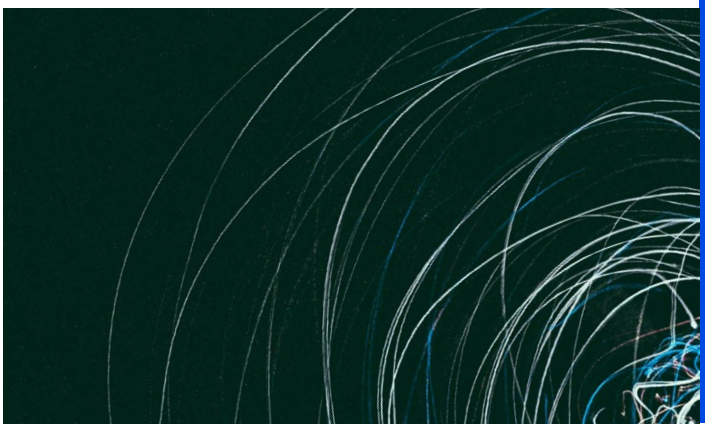
This policy brief argues that legislation enabling data trust through a regulatory sandbox scheme can provide powerful insight into how these conflicting goals can be reconciled paving the way for a fair, competitive, and safe data economy.

BACKGROUND

The explosive growth of artificial intelligence (AI) has been driven by the massive increase in available data, along with increased computer storage capacity, processing power, and data transmission speed.

It is estimated that by 2030 there will be over 29 billion connected Internet of things (IoT) devices generating data. Much of this data is collected and controlled by some of the largest corporations in the world. The speed with which ChatGPT has been adopted is without precedent, with over 100 million users engaging with the app in its first two months. **Although the EU has been at the forefront of data protection, it is impossible for any government to anticipate and regulate for all desired outcomes due to the speed with which emerging technologies are advancing.**

The harms to data subjects from reckless data use are well documented as is the need for the legal and ethical data sharing. However, strict limits on data use and sharing in the form of legislation have had a detrimental effect on innovation, particularly with respect to start-ups and SMEs. In fact, some have argued that restrictions can have the perverse effect of concentrating power in the hands of Big Tech. Even organizations that would be willing to share their data may be reluctant to do so because of concerns about the legal risks of doing so. Moreover, while these laws give data subjects the right to control their data, those whose rights are violated find it difficult to bring private lawsuits without financial backing, and data protection authorities charged with enforcing data protection laws are both understaffed and underfunded.



What is needed is a flexible governance device that can help find the best way to enable data sharing while protecting data subjects.

A balance that can only be achieved on a decentralized, case-by-case basis, not through one-size-fits-all regulation. The device that is the subject of this report is **data trust**.

LEGAL REGIME

In the U.S., where most of Big Tech is based, there is no national privacy law. The U.S. relies primarily on voluntary initiatives, sector-specific regulation, and state laws. This is why tech companies in the U.S. have grown into behemoths, but it is also why there have been significant data breaches. In contrast to the U.S., the EU has developed a data use strategy with comprehensive legislation on the use of personal data, data transfers, and the risks of artificial intelligence. This approach begins with the General Data Protection Regulation (GDPR) privacy rules, which give data subjects control over their data. More recently, as part of the EU's Data Strategy, a series of regulations and directives have sought to both further protect data subjects from automated decision-making (AI Act) and encourage data sharing by companies that collect and process data (Data Governance Act and Data Act). However, despite their intent and importance, these laws present obstacles to the use of data trusts.

DATA TRUST

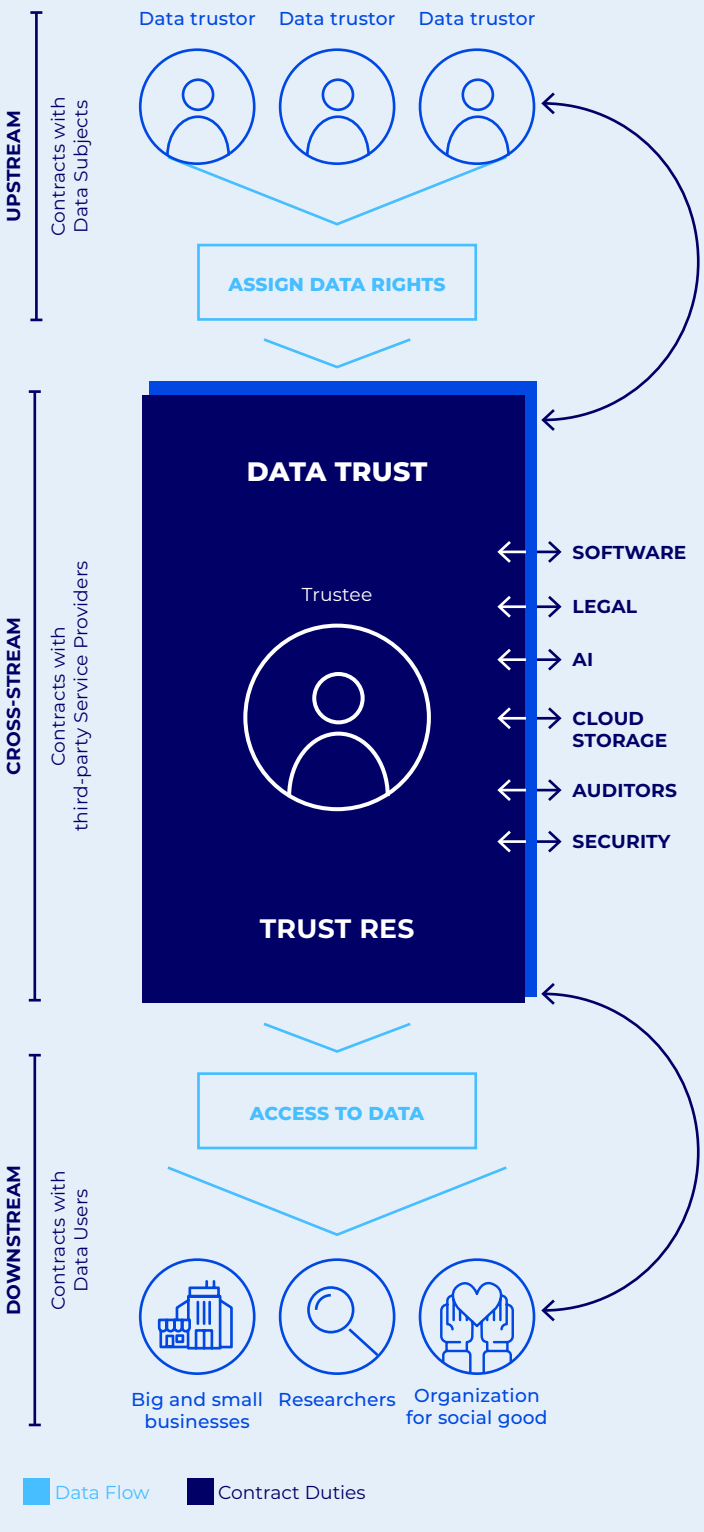
There is no universally accepted definition of a data trust. In fact, there are a number of organizations that use the term that have nothing to do with data protection. There is also disagreement as to whether data trusts operate under trust law, which imposes a fiduciary duty on the trustee, or under contract law, which requires good faith. In fact, some scholars have argued that it is unlikely that data trusts could be viable under trust law because **(1)** a trust requires a *res* and data may not be considered property, and **(2)** trust law imposes a fiduciary duty on the trustee that could prohibit the sharing of data for business purposes. A more flexible iteration of a data trust would be one designed using a stewardship model.[2] Although it has legal and technical elements, a data trust is first and foremost a governance structure.

A data trust can be viewed as a collection of relationships with a trustee's duty falling somewhere between strict fiduciary requirements and the minimal good faith requirements found under contract law; in essence, a stewardship model.

- Data subjects would first assign their data rights to the trustee (upstream relationship).
- The trustee would then be authorized to arrange for the necessary services associated with the trust, such as accounting, legal, storage, cybersecurity, etc. (cross-stream relationship).[3]
- Ultimately, the trustee would negotiate agreements for the use of the data by third parties based on the trust's purpose allowing the pooled data to be used for social good and/or private innovation (downstream relationship).

For example, a trust could be designed to accumulate data from household water usage in a community for the purpose of anticipating potential shortages (social good) or for use by an SME developing a new type of app which permits a resident to monitor their own water usage (private innovation).

FIGURE 1: Data Trust configuration[4]



CURRENT LEGAL RESTRICTIONS

Although data trusts are promising, there are a number of legal obstacles standing in the way of their use.

For example, with respect to upstream agreements, the GDPR, which applies to personal data, does not specifically permit data subjects to delegate their rights except in the case of filing a complaint with a supervisory authority.[5] Additionally, the Data Governance Act (DGA) indicates that data rights "are personal rights of the data subject."[6] This would appear to prevent data subjects from appointing a trustee to make decisions and exercise data rights on their behalf. Additionally, with respect to downstream agreements, the GDPR presents enormous risks with respect to the sharing of data with third parties due to potential liability concerns for third party uses.

One of the ways that the EU is attempting to encourage the sharing of data for both commercial and social good is through the conceptualization of data intermediaries and data altruism as provided in the DGA. The recently enacted Data Act[7] and the Data Governance Act (DGA)[8] were designed to, among other things, promote data sharing as part of the European Data Strategy.[9] The Data Act facilitates the sharing of industrial data for the benefit of government and SMEs. However, it has been heavily criticized for putting further restriction on cross-border transfers, potential conflicts with the requirements of the GDPR, and lack of attention to protecting trade secrets.

The DGA provides a licensing mechanism for data intermediaries, along with strict requirements and penalties for noncompliance. Although on the surface this legislation appears to permit data trusts, there are a number of provisions that make data trusts unviable. For example, Art. 12(a) provides that intermediaries may not use the data "for any purpose other than to make it available to the data users". It is unclear whether this means intermediary purposes or "lawful purposes" as described in the GDPR. In fact, it may be that the provision contemplates single-purpose devices. If that is the case, the cost of building and maintaining the trust in compliance with all of the legal and technical requirements of the DGA would not be justified.

A data trust needs the flexibility to share data with multiple parties for their varying uses as long as such uses are in alignment with the trust's purpose.

The DGA could also limit the trustee's ability to act on behalf of data subjects in unanticipated ways. Recital 33 of the DGA appears to impose a fiduciary duty on intermediaries which may prevent data use for commercial purposes because a fiduciary is required to act solely for the benef it of the data users. A data trust envisions a balancing between the needs of the data subjects and the data users under a stewardship arrangement. Despite the promise of EU's data intermediaries and other data sharing initiatives, there are still a number of prohibitive conflicts and uncertainties under current EU law which would impede the widespread use of data trusts.

CURRENT LEGAL RESTRICTIONS

Overall, a data trust can address the many issues arising from less formal (and more formal) data sharing mechanisms.

01 First, it would operate with the consent of the data subjects, but not require input into every decision on data use such as with a data cooperative.

02 Second, by being able to monetize the pooled data, it could provide the necessary funds for the ancillary services needed to operate the trust and protect the data.

03 Third, a trustee's expertise in data protection would avoid the risks that data subjects may encounter with the use of their data by unknown entities.

04 Fourth, the exact nature of the stewardship would be spelled out in the trust document rather than relying on common law and restrictive regulations regarding intermediaries.

05 Fifth, by designating the purpose of the trust (e.g., sharing data for medical research [social good] and/or developing medical devices [private good]), the need to obtain ongoing consent for each and every use of the data would be obviated.

Because of the lack of explicit authorization for these stewardship devices in the EU, **a new regime is needed to test and facilitate their use.**

TOWARDS SOLUTIONS: SANDBOXES

As discussed above, the ability to operationalize a flexible, stewardship-style data trust is unlikely under current law. However, simply amending the DGA to include data trusts is not enough. In order to provide data users with access to data sets, protect data subjects from harmful uses of their data, and at the same time identify best practices, a legal sandbox for data trusts should be established as part of the EU's data strategy.

A regulatory sandbox can provide valuable information to regulators on how this model could be used PRIOR to creating regulations for its use.

Although sandboxes have historically been found in FinTech, they are gaining traction around the world as an incredibly effective device. The UK Financial Conduct Authority (FCA) is believed to have created the first formal regulatory sandbox which it defines as "a 'safe space' in which businesses can test innovative products, services, business models and delivery mechanisms without immediately incurring all the normal regulatory consequences of engaging in the activity in question."[10] The transparency required of such organizations permits regulators to see how the new product, service or model works in practice to determine the risks and best practices. This ability prevents legislators from creating unworkable *ex ante* regulations that have unanticipated consequences or become obsolete before the law's effective date.

Regulatory sandboxes can provide enormous insight into how a new technology operates which guides both the organizations in the sandbox and the regulators observing the sandbox.[11]

Enabling regulations for a data trust sandbox would need to permit the delegation of data subject rights to a trustee and provide very flexible guidelines for the creation of the trust under a stewardship model.

In December 2023, the European Supervisory Authorities (ESA) released its 2023 Joint Report on innovation hubs and regulatory sandboxes which sets out best practices and other discoveries from the various sandboxes monitored.[12] Additionally, the European Commission has also created a set of guidelines in setting up regulatory sandboxes.[13] Article 53 of the AI Act anticipates the use of these regulatory structures in which to test out AI systems demonstrating an openness to these types of testing grounds beyond specific industries.

CONCLUSION

European innovation and the growth of the data economy require legal certainty, clear guidance, and the ability to experiment with new data sharing mechanisms without fear of fines and litigation. However, these new mechanisms must protect data subjects and allow data to be shared with those who can use it for public, social and private good. Enabling data trusts under a stewardship model is ideal because:

01 Organizations (data users) can contract with a data trust trustee who would be responsible for legal compliance with data sharing and data protection law.

02 Trustees operating under a stewardship model would provide a certain level of trust to those who provide their data to the trust (data subjects).

Rather than trying to anticipate in advance how a data trust should work and how it fits within current law, a data trust sandbox would permit the testing of data trusts and provide important information for designing a workable regulatory scheme around data sharing.

By allowing the testing of data trusts in the EU under appropriate national competent authorities, enormous value could be gained by regulators in understanding of how regulations should be crafted to better balance the rights of data subjects with the need for data sharing.

A data trust may be the answer to unlocking the incredible value that data holds while supporting a data economy that is fair, competitive, and safe.

ENDNOTES

1 OECD Studies on SMEs and Entrepreneurship (2024).

2 Kimberly A. Houser & John W. Bagby, *Next-Generation Data Governance*, 21 DUKE L. & TECH. REV. 61, 95-98 (2024).

3 Kimberly A. Houser & John W. Bagby, *The Data Trust Solution to Data Sharing Problems*, 25 VAND. J. ENT. & TECH. L. 113, 153 (2023).

4 Houser & Bagby, *The Data Trust Solution*, at 155 (2023).

5 Regulation 2016/679 of 27 April 2016 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) 1 (May 4, 2016) Art. 80.

6 Commission Regulation 2022/868 of May 30, 2022, European Data Governance and Amending Regulation (EU) 2018/1724, annex, 202 O.J. (L 152) 1 (Data Governance Act [DGA]) Recital 31.

7 *Commission Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data*, COM (2022) 68 final (Feb. 23, 2022).

8 Commission Regulation 2022/868 of May 30, 2022, European Data Governance and Amending Regulation (EU) 2018/1724, annex, 202 O.J. (L 152) 1. (Data Governance Act ('DGA').

9 *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM (2020) 66 final (Feb. 19, 2020).

10 UK Financial Conduct Authority, Regulatory Sandbox (Nov. 2015).

11 Federal Ministry for Economic Affairs and Energy, Making Space for Innovation—The Handbook for Regulatory Sandboxes (2019).

12 ESA 2023 27 (11 December 2023), https://rb.gy/3k3oye.

13 See 'TOOL #69. Emerging methods and policy instruments', pages 599-604, https://rb.gy/w9hgw0

ie UNIVERSITY

CENTER FOR THE GOVERNANCE OF CHANGE

This policy brief was produced within the framework of the Center for the Governance of Change's research program *The Digital Revolution and the New Social Contract*, and in particular its second work package, which studies the emergence and governance of the data economy, and how it can be fair, competitive, and safe.

You can access the paper and learn more about the program here:
https://www.ie.edu/cgc/research/new-social-contract-digital-age

© 2024, CGC Madrid, Spain

Design: epoqstudio.com
Images: Unsplash and Shutterstock

This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License. To view a copy of the license, visit creativecommons.org/licenses/by-nc-sa/4.0

cgc.ie.edu