

Enabling data sharing for social benefit through data trusts

An Interim Report for the 2021 GPAI Paris Summit

Produced by:



aapti institute



In collaboration with:



GPAI |

THE GLOBAL PARTNERSHIP
ON ARTIFICIAL INTELLIGENCE

The outputs of this interim report have been developed by the Aapti Institute (output 1 and 2) and Open Data Institute (output 1) for consultation. It has been commissioned by experts of the Global Partnership on AI and does not necessarily reflect the views of the experts' organizations, GPAI, the OECD or their respective members.

Table of Contents

Introduction.....5

Output 1: Data trusts global survey.....7

Output 2: Legal Review.....47

Introduction



Neil Lawrence

Co-Lead, GPAL's Data Trusts project
DeepMind Professor of Deep Learning
University of Cambridge



Seongtak Oh

Co-Lead, GPAL's Data Trusts project
Vice President
National Information Society Agency

Data trusts: a new paradigm in data stewardship

Earlier this year, GPAL's Data Governance Working Group launched its new project Enabling data sharing for social benefit through data trusts. This project set out to help realise the potential of data trusts as a mechanism for trustworthy data sharing, by advancing research and practice that supports the creation of real-world data trusts.

Data trusts are a type of data institution that allows individuals or groups to pool resources, tasking an independent 'trustee' to manage those resources for the benefit of the trust's members. While the specific motivations of those setting up a data trust will vary in different contexts, data trusts are characterised by their focus on:

- enabling data-driven innovation for social and economic benefit, by creating a trustworthy environment for data sharing.
- re-balancing power asymmetries in data exchanges, by encouraging and empowering the originators of the data to play an active role in setting the terms of data use – and the distribution of the value that creates – and providing a platform for collective negotiation; and
- anticipating, preventing, and managing the vulnerabilities associated with data use, through professional data stewardship.

In a statement earlier this year, GPAL set out some of the core functions of data trusts, based on discussions amongst Working Group members.¹ This explored the distinctive contribution that data trusts can make to data stewardship: by offering a vehicle for individuals or groups to choose how they want data about them to be used and engaging a trustee to act for their benefit, data trusts can provide a mechanism for bottom-up engagement that empowers individuals and communities in decisions about data use. That statement also highlighted some of the challenges associated with creating real-world data trusts: from identifying community needs to creating strategies for implementation.

To help understand current strategies for operationalising data trusts and the role of different legal frameworks enabling their development, GPAL has commissioned the Aapti Institute and the Open Data

¹ These functions are: provide a platform for collectives to establish desirable terms and conditions of data use, setting the constitution of a trust; appoint expert trustees (professional managers) to take responsibility for the stewardship of the trust's assets, create a regime of strong fiduciary responsibilities to bind the trustees to act in the interests of the trust's members; negotiate use of trust assets in accordance with agreed terms and conditions, facilitating safe and controlled data use; and establish safeguards and oversight mechanisms to prevent data misuse and to take remedial action in the event of the trust's terms and conditions being breached.

Institute (ODI) to produce two new reports, now published for consultation. A survey of current data trust projects by the ODI and Aapti Institute collates experiences from 45 practitioners and researchers, presenting their views on what functions data trusts are delivering and what operational strategies help deliver them. In parallel, the Aapti Institute's review of legal frameworks synthesises recent legal and policy developments surrounding data trusts, comparing the experiences of 11 different jurisdictions.

We hope these reports will contribute to a continuing conversation about the potential of data trusts in enabling data sharing for social benefit. To support that dialogue, this summary presents key messages from these two interim outputs.

Lessons from current practice

A community of research and practice is already growing around data trusts. This community is trialling alternative approaches to data stewardship, with the aim of empowering individuals and communities. It is also changing and growing at pace, as new projects start up and grow – 80% of projects surveyed were less than 5 years old or yet to be operational – and as research and policy debates evolve.

While the last few years might have been characterised by a proliferation of projects using the term 'data trust' in different ways, survey responses suggest that the community is moving towards a shared understanding of what data trusts are, and how they differ from other forms of stewardship. 82% of respondents agreed with the definition of data trusts that GPAI [proposed in our statement earlier this year](#). Those disagreeing raised helpful questions about how terms like 'data producers' and 'fiduciary duties' will be interpreted in different contexts, but were broadly in alignment with the idea that data trusts play a distinctive role in creating an environment for enhanced accountability, while empowering individuals and communities.

The review of working practices produced by the ODI and Aapti Institute highlights a range of innovations in stewardship practice that are being used by different initiatives to operationalise data trusts:

- Practitioners are using different legal frameworks, including limited companies, foundations, non-profits, and cooperatives, adapting to the opportunities and challenges associated with the legal environment in which they operate.
- Technologies being deployed to manage data vary across projects, with examples of data 'pods', 'vaults', 'personal data stores' and distributed ledger-based services playing a role in operationalising data management strategies. Practitioners also highlighted the role that Application Programming Interfaces play in helping connect data across organisations and the potential for privacy enhancing technologies to support the wider data sharing ecosystem.
- Different business models are emerging from efforts to make current projects financially sustainable over the long-term. While many early-stage projects are reliant on philanthropic funding, public funding, private investment – or other non-earned revenue streams – other emerging business models use membership fees, data access fees, or data insights packages to generate revenue.
- With the aim of facilitating bottom-up engagement in decisions about data use, initiatives have been developing different forms of participatory and delegated decision-making. These span a spectrum from individual-focused (for example, seeking consent from individual members to include – or withdraw – their data from specific use cases), to cooperative negotiations.

This diversity of practices is allowing projects to deliver many of the core functions of a data trust, while adapting to local conditions. Projects included in this review typically reported delivering four or five of the six core data trust functions, with many focusing on providing a platform to pool data while establishing safeguards and oversight mechanisms around data use. In one area, however, a clear gap is emerging between theory and practice: the role of trustees in enabling data stewardship remains a difficult aspect of data trusts to operationalise. With trustees expected to play an important role in increasing accountability and enforcing safeguards around data use, this gap has implications for both how data trusts can work today, and how the field might develop in future.

Implications for policymakers

The Aapti Institute's review of global legal frameworks also highlights a diversity of policy approaches towards data stewardship across the globe. Countries differ in: the extent to which their current legislation provides data rights for individuals or communities, the ways in which those rights – where they exist – can be enacted through data institutions; and in their ability to support or enforce fiduciary relationships between parties in a data sharing arrangement.

Examining how legislation can facilitate data stewardship and bottom-up empowerment, this interim report identifies three legislative building blocks for data trusts and other data intermediaries. These are:

- **Data rights and protections:** Data trusts are a tool to help citizens enact their rights; a prerequisite for their operationalisation is the existence of clear and robust data rights within a jurisdiction. These rights might include data portability, findability, and accessibility – legal provisions that give individuals rights over use of data about them – and may need to be extended to include rights around community data or co-generated data. If data trusts are to operate effectively, these rights also need to be managed in a way that allows the trustee to act on behalf of the trust's members, raising legal questions about how to delegate or mandate rights to a trust.
- **Data sharing policies:** A range of different legal agreements and frameworks play a role in supporting the data sharing ecosystem in which data trusts operate. Some of these are explored in the interim report, including data standards, data formats, sector-specific policy frameworks and other data sharing agreements. The ability of data trusts to facilitate data use will depend in part on the effectiveness of this wider environment.
- **Fiduciary obligations:** Definitions of fiduciary responsibilities vary across countries. Under common law, fiduciary duties can be used to create safeguards around data trusts – they would require data trustees to act in the best interests of the trust's members, and are associated with high levels of accountability and loyalty for those trustees. In other jurisdictions, different strategies will be needed to implement such requirements, ensuring data trusts remain trustworthy. Such actions may include regulation, opportunities for judicial intervention, or other policy action.

Recent years have already seen attempts by governments to develop policy or regulatory frameworks that can facilitate the development of data intermediaries. While the framework presented in the Aapti Institute's report is still in development, policymakers can look to these building blocks as a framework for assessing data trust-readiness. Important questions to consider in the next phase of developing the policy environment will include:

- Are existing data rights sufficient?
- What types of data sharing infrastructure are needed to underpin data trusts?
- Do existing legal frameworks provide sufficient safeguards to ensure data trusts remain trustworthy?

Next steps

Together, these interim reviews show both the progress that has been made in advancing data trust research and practice over the last five years, and the progress that is needed to operationalise the vision behind data trusts. They raise interesting questions at the interface of data trust research and practice, including:

- What support do practitioners need to operationalise real-world data trusts? What new operational strategies can help deliver all the core functions of data trusts?
- In what areas are there significant, unrealised opportunities for creating data trusts that benefit people and society?
- What data rights and data sharing infrastructures must be in place to enable data trusts to operate? Where legal interventions are not available, what alternative strategies can work in their place?
- What interventions can help ensure that data trusts remain trustworthy? As our understanding of core concepts – like fiduciary responsibilities, co-generated rights and collective interests around data use – evolves, what changes to legal or operational frameworks might be needed?

Part of the appeal of data trusts as a stewardship model is their flexibility – their ability to adapt to local needs and opportunities. The diversity of working practices and policy approaches explored in the interim reports that GPAI is publishing today in collaboration with the Aapti Institute and ODI offer opportunities for taking stock of what the data trusts community has learned so far, and how it might continue to develop in future.

These reports are the first outputs from GPAI's data trusts workstrand. In the coming months, we'll continue to work with the Aapti Institute and the Open Data Institute to refine their findings and identify the lessons that can inform future practice and policy development. We hope they can start a conversation with the data trusts community – if you'd like to provide feedback on the reports, please get in touch via info@ceimia.org.

If successful, data trusts could fill an important gap in the data stewardship landscape. By providing a space for meaningful community engagement and participation, they could help connect our aspirations for data sharing for social good with the imperative to avoid the harms associated with untrustworthy data use. We look forward to hearing your views about what we can learn from experiences of creating data trusts so far, and how the community might develop in future.

Output 1: Data trusts global survey

Produced by:



In collaboration with:



Table of Content

<i>Executive Summary</i>	11
<i>The emergence of data trusts</i>	12
1.1. Data stewardship	12
1.2. Bottom-up data stewardship	14
1.3. Data trusts: an evolving conceptual framework	16
1.4. Differing interpretations of data trusts	17
1.5. Institutionalising data trusts and codifying fiduciary responsibilities	18
2. International knowledge, attitudes and practices of data trusts	22
2.1. Context	22
2.2. Awareness and understanding.....	23
2.3. Practices.....	24
2.4. Attitudes towards data trusts	27
3. Case studies	28
3.1. Criteria and selection.....	28
3.2 Driver’s Seat	29
3.3. Open Humans.....	32
3.4. MIDATA	34
3.5 Insights from case studies.....	36
4. Key findings and takeaways	37
5. Endnotes	38
5.1 About Aapti, ODI, and GPAI	38
5.2 Authors	38
5.3 Report drafting.....	38
5.4 Acknowledgements	38
6. Bibliography	39
6.1 Review of literature (academic papers, blogs, comments, news reports)	39
6.2 Policy, regulation and strategy documents.....	45
6.3 Tools, guides and videos.....	45

Executive Summary

Progress in artificial intelligence (AI) requires access to data. Who shares data, for what purposes and under what conditions will therefore shape the development of AI and the challenges it is put to.

However, many organisations currently regard data as something to hoard, causing it to be inaccessible to those who could otherwise use it to create new products or insights. At the same time, **a lack of involvement of individuals and communities in shaping how data is used will deny beneficial uses of data**, due to people withdrawing their consent - in the broad sense - for its collection and sharing.

In response, **data stewardship** has emerged as a responsible, rights-preserving and participatory concept. It aims to unlock the economic and societal value of data, while upholding the rights of individuals and communities to participate in decisions relating to its collection, management and use.

In this context, **this research set out to understand global knowledge, attitudes and practices of data trusts.** It was undertaken for the Global Partnership on AI (GPAI) by Aapti and the Open Data Institute between August and October 2021, using a combination of literature review, survey and case studies. It adopted the GPAI's Data Governance Working Group interpretation of data trusts as:

“a form of data stewardship that supports data producers to pool their data (or data rights) with the aim of collectively negotiating terms of use with potential data users, through the oversight by independent trustees, with fiduciary duties, and within a framework of technical, legal and policy interventions that facilitate data use and provide strong safeguards against mis-use”.

The project's literature review (Section 2) found significant theory, interest and experimentation around new forms of 'bottom-up' data stewardship that seek to empower people to participate in the process of data collection, use and sharing. The analysis frames data trusts as a particular, evolving form of bottom-up data stewardship. It found emerging consensus on distinctive features of data trusts and that practitioners deploy a variety of operational strategies to realise its functions.

A survey (Section 3) was completed by 45 people building or running data trusts and similar bottom-up data stewardship initiatives, or who are working on data stewardship and related topics. Analysis of the survey (summarised in Section 5) found that:

- **today's data stewardship projects deliver many of the functions associated with data trusts**, but delivering all the functions attributed to a data trust, as per the GPAI Data Governance Working Group's interpretation, remains a challenge
- there is general optimism about the potential of data trusts among people working on data stewardship.
- the interest in data trusts as a form of data stewardship seems to be concentrated in Europe and North America.
- There are a number of real-world initiatives that demonstrate multiple routes to realising bottom-up data stewardship that do not follow the data-trust definition or deliver all of the functions associated with data trusts.
- The **purpose for bottom-up data stewardship can differ significantly**, from supporting altruism to generating commercial return and this defines how models design their governance mechanisms.

The case studies (Section 4) document three bottom-up data stewardship initiatives: Driver's Seat, Open Humans and MIDATA. They represent **real-world examples of how groups can be empowered around data they've generated** and are actively making available data for broad societal benefit.

The intent is for this report to act as a reference point on the subject of data trusts for practitioners seeking inspiration, as well as policymakers, funders and other enabling actors considering how to support the field.

The emergence of data trusts

- This section presents a review of literature on data stewardship and the evolution of the concept of data trusts, discussing the work of Sylvie Delacroix and Neil Lawrence, Sean McDonald and other scholars, and organisations such as the Mozilla Data Futures Lab and the Ada Lovelace Institute.
- The review documents significant theory, interest and experimentation around new forms of 'bottom-up' data stewardship that seek to empower people to participate in the process of data collection, use and sharing.
- The review frames data trusts as a particular, evolving form of bottom-up data stewardship, and found rapid proliferation around the use of the term among practitioners and scholars of stewardship.
- While there is divergent opinion from around the world on how data trusts could be constructed, the stewardship community is nevertheless working to consolidate their understanding of the term.

1.1. Data stewardship

The effective collection, use and sharing of data can help address the pressing challenges of our time - from surfacing remedies for climate change² to improving public health³.

The transformative power of data is best explained through the lens of examples such as the Human Genome Project, undertaken between 1990 and 2003.⁴ Led by the US Government's National Institute of Health, the Project made available data on DNA sequencing within 24 hours of its discovery. The consequent availability of that data for research and development has not only saved lives, but also generated \$796 billion in economic impact and supported over 300,000 jobs in 2010 alone.⁵ More recently, the same data sharing norms established by the Human Genome Project (the 'Bermuda principle'⁶) were adopted in the development of vaccines against SARS-COV-2.⁷ A lab in China released the genome sequence of the coronavirus in January 2020, which was subsequently used by researchers around the world to develop antidotes, even without access to physical genomic samples of the virus.

However, despite the positive benefits of data, the emergence of new approaches to its collection, use and sharing - particularly driven by developments in machine learning⁸ - is underpinned by two disconcerting trends.

2 Szasz, Open Data Institute (2020), "Tackling Climate Challenges through Data Access: Microsoft and the ODI", <https://theodi.org/article/tackling-climate-change-challenges-through-data-access-microsoft-and-the-odi/>

3 Harper, International Journal of Infectious Diseases (2016), "Sharing Public Health Data Saves Lives", [https://www.ijidonline.com/article/S1201-9712\(16\)31285-1/fulltext](https://www.ijidonline.com/article/S1201-9712(16)31285-1/fulltext)

4 See <https://www.genome.gov/human-genome-project/What>

5 Tripp and Greuber, Battelle Memorial Institute (2011), "Economic Impact of the Human Genome Project", <https://www.battelle.org/docs/default-source/misc/battelle-2011-misc-economic-impact-human-genome-project.pdf?sfvrsn=6>

6 See <https://dukespace.lib.duke.edu/dspace/handle/10161/7407>

7 First and Collins, Forbes (2021), "NIH Director Dr. Francis Collins: Connecting The Dots From The Human Genome Project To The COVID-19 Vaccine", <https://www.forbes.com/sites/billfrist/2021/01/20/nih-director-dr-francis-collins-connecting-the-dots-from-the-human-genome-project-to-the-covid-19-vaccine/?sh=738447175438> [Podcast]

8 Expert Panel, Forbes Technology Council (2019), "15 Social Challenges AI Could Help Solve", <https://www.forbes.com/sites/forbestechcouncil/2019/09/03/15-social-challenges-ai-could-help-solve/?sh=76e9dd973533>

First, the market-driven imperatives of corporations have helped create digital enclosures⁹ that hampers the ability to use data for broad-based social benefit. Much of the current data economy is defined by a paradigm of extraction¹⁰, whereby the role of individuals and communities as the generators of data goes unrecognised.¹¹ This process has been described variously as the “attention economy”,¹² “surveillance capitalism”¹³ and “computational capitalism”¹⁴, with corporations’ use of data existing beyond the control of those individuals and communities.¹⁵ For instance, patients signing-up to digital health applications have little knowledge of who has access to their data and how it will be used,¹⁶ just as rideshare drivers in the gig economy are excluded from the management of algorithms that govern their work.¹⁷

Second, a lack of consideration of ethics and equity, and a lack of engagement with those affected by data’s use, undermines trust in the process of data sharing. In the UK, the Government came under scrutiny for its GP Data for Planning and Research (GDPDR) proposal, which would facilitate access to the health records of 55 million people.¹⁸ The proposal has been indefinitely postponed, having been subject to criticism for not giving patients a meaningful say in how the system should work.¹⁹ Equally, high profile data breaches such as the 2017 Equifax data breach, where an unauthorized third party gained access to data on as many as 143 million Americans, serve to erode the trust we have as consumers in the processing of data about us.²⁰

These trends have given rise to inter-related phenomena - ‘data hoarding’ and ‘data fearing’²¹. ‘Data hoarding’ relates to a scenario where organisations restrict access to data due to misperceptions about its value to their operations or the risks associated with data sharing. The benefits of data collection and use would only be enjoyed by a few, while the negative impacts of its use would affect society as a whole.²² On the other end is the scenario of ‘data fearing’, where data might not be collected or used to the extent it could, due to concerns about the harm that it can cause people being left unaddressed. People might avoid using services, or withdraw consent for data to be collected, which means that we end up missing data and the uses of it that could support human flourishing.

The concept of data stewardship is a response to these ‘data hoarding’ and ‘data fearing’ scenarios. Data stewardship can be understood as an approach to data governance that is responsible, rights-preserving and participatory in nature²³. In effect, data stewardship aims to unlock the societal value of data, while upholding the data rights of individuals and communities to participate in decisions relating to its collection, management and use.²⁴

9 Andrejevic (2009), Amsterdam Law Forum, “Privacy, Exploitation and the Digital Enclosure”,

https://www.researchgate.net/publication/228226821_Privacy_Exploitation_and_the_Digital_Enclosure

10 Morozov, E., (n.d.), Council of Europe, “Digital Intermediation of Everything: At the Intersection of Politics, Technology and Finance”, <https://rm.coe.int/digital-intermediation-of-everything-at-the-intersection-of-politics-t/168075baba>

11 Manohar, Kapoor and Ramesh (2020), Aapti Institute, “Data Stewardship: A Taxonomy”, <https://thedataeconomylab.com/2020/06/24/data-stewardship-a-taxonomy/>

12 Beuno (2017), London: Rowman and Littlefield International, “The Attention Economy: Labour, Time and Power in Cognitive Capitalism”

13 Zuboff (2018), New York: PublicAffairs, “The Age of Surveillance Capitalism: The Fight for Human Future at the New Frontier of Power”

14 Beller (2018), London: Pluto Press, “The Message is Murder: Substrates of computational capital”

15 Lawrence (2016), The Guardian, “Data trusts could allay our privacy fears”, <https://www.theguardian.com/media-network/2016/jun/03/data-trusts-privacy-fears-feudalism-democracy>

16 Sur (2021), Medianama, “Online medical platforms are playing fast and loose, collecting patient data”, <https://www.medianama.com/2021/09/223-india-digital-health-medical-platforms-data-consent-records/>

17 O’Connor (2016), Financial Times, “When your boss is an algorithm”, <https://www.ft.com/content/88fdc58e-754f-11e6-b60a-de4532d5ea35>

18 Vallance (2021), BBC News, “GP Data Sharing: What is it and can I opt out?”, <https://www.bbc.com/news/technology-57555013>

19 Crouch (2021), Digital Health, “GP Data September implementation data is scrapped”, <https://www.digitalhealth.net/2021/07/gpdr-september-implementation-date-scrapped/>

20 Forbes (2017), “Equifax Data Breach Impacts 143 Million Americans”, <https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/#6f6ed8d3356f>

21 Open Data Institute (2021), “What are data institutions and why are they important?”, <https://theodi.org/article/what-are-data-institutions-and-why-are-they-important/>

22 Newman (n.d.), Federal Trade Commission, “How Big Tech enables harms to consumers, especially to low-income and other vulnerable sectors of the population”, https://www.ftc.gov/system/files/documents/public_comments/2014/08/00015-92370.pdf

23 Ada Lovelace Institute (2021), “Disambiguating data stewardship”, <https://www.adalovelaceinstitute.org/blog/disambiguating-data-stewardship/>

24 Manohar (2019), Aapti Institute, “Responsible data sharing for public good: Theoretical bases and policy tools”, <https://thedataeconomylab.com/2020/07/31/data-sharing-for-public-good-theoretical-bases-and-policy-tools/>

1.2. Bottom-up data stewardship

Corporations, governments and civil society organisations find themselves occupying powerful positions in determining how data is put to use. However, within most current mechanisms for data collection, use and sharing, the involvement of individuals and communities is non-existent.

In response, a more empowering paradigm of ‘bottom-up data stewardship’ has emerged. It builds on the ideals of data stewardship, recognising individuals and communities as more than recipients of information - or mere providers of consent - about how data about them is used²⁵, and seeks to empower them to participate in the process of data collection, use and sharing.

An ecosystem of research and practice has emerged around this concept of ‘bottom-up data stewardship’. The MyData Global community, for example, is set out “to empower individuals by improving their right to self-determination regarding their personal data”²⁶. The Mozilla Data Futures Lab was launched in 2021 to support experimentation around “new approaches to data stewardship that give greater control and agency to people”²⁷. The Ada Lovelace Institute advocates for ‘participatory data stewardship’, where people whose data is used or about which data decisions are taken are meaningfully involved.²⁸ Aapti Institute’s work at the Data Economy Lab²⁹ aims to empower individuals and communities to play a bigger part in data governance, and it has documented numerous examples of this in practice.³⁰

Research suggests that the bottom-up data stewardship initiatives emerging from this ecosystem can be functionally very different, especially in terms of the types of involvement they afford to individuals and communities³¹. Some initiatives - such as Bitsabout.me³² - enable people to make granular, individual decisions about who has access to data about them, for what purposes and in exchange for what;³³ other initiatives - such as Salus.coop³⁴ and others described below - enable people to participate in collective decision-making as part of a community;³⁵ and a few initiatives - such as Jumbo³⁶ - enable people to delegate another party to mediate data collection and use.³⁷ Research on bottom-up data stewardship has also demonstrated the array of other ways such initiatives can differ.³⁸ Aapti’s Stewardship Mapper³⁹, which draws on interviews and analysis of 100+ bottom-up data stewardship initiatives, describes nine categories of ‘design choices’ practitioners can make in constituting them, from business models to technical features.

In particular, a number of promising initiatives have emerged to enable groups to generate or repurpose data about them, and exert collective control over it for a common purpose. For instance:

- Variant Bio⁴⁰ works with historically marginalised populations to facilitate people-driven therapeutics. Communities are engaged prior to the beginning of research projects; their data is then collected and used within a framework that focalises community concerns.

25 Ada Lovelace Institute (2021), “Participatory data stewardship: A framework for involving people in the use of data”, <https://www.adalovelaceinstitute.org/report/participatory-data-stewardship/>

26 MyData (n.d.). Retrieved from <https://mydata.org/>

27 Mozilla (n.d.). Retrieved from <https://foundation.mozilla.org/en/data-futures-lab/>

28 Ada Lovelace Institute (2021). Retrieved from <https://www.adalovelaceinstitute.org/event/exploring-participatory-mechanisms-data-stewardship-report-launch/>

29 Aapti Institute (2021). Retrieved from <https://thedataeconomylab.com/>

30 Aapti Institute (2021). Retrieved from <https://thedataeconomylab.com/tracking-stewardship/>

31 Hardinges and Keller (2021), The Open Data Institute, “What are “bottom-up” data institutions and how do they empower people?” <https://theodi.org/article/what-are-bottom-up-data-institutions-and-how-do-they-empower-people/>

32 BitsaboutMe (2021). Retrieved from <https://bitsabout.me/en/>

33 Digime (2021). Retrieved from <https://digi.me/> ; Schluss Foundation (2021). Retrieved from <https://schluss.org/>

34 Salus Coop (2021). Retrieved from <https://www.saluscoop.org>

35 LunaPBC (2021). Retrieved from <https://www.lunadna.com/> ; Open Data Manchester (n.d.). Retrieved from <https://www.opendatamanchester.org.uk/>

36 Dumbo (2021). Retrieved from: <https://www.withjumbo.com/>

37 Ciitizen Corporation (2021). Retrieved from <https://www.ciitizen.com/> ; UTS-CRiCOS (2021). Retrieved from <https://www.ciitizen.com/>

38 Sridharan, Kapoor & Manohar (2021), “Health data stewardship: Learning from use cases”, <https://thedataeconomylab.com/2021/09/29/health-data-stewardship-learning-from-use-cases/>

39 Aapti Institute (2021). Retrieved from <https://thedataeconomylab.com/mindmap/>

40 Variant Bio (2021). Retrieved from <https://www.variantbio.com/>

- Driver's Seat⁴¹ is an independent, driver-owned cooperative where members' data is used to derive insights that help them optimise their performance.
- Swash⁴² enables users to control what data is collected about their browsing habits, as well as aggregate and sell access to this data to generate financial return.
- OpenHumans⁴³ empowers individuals and communities to explore and share their personal data for the purposes of education, health and research.
- MIDATA⁴⁴ enables users to contribute to medical research and clinical studies by granting selective access to their personal data.
- Gyeonggi Data Dividend⁴⁵ ensures that any financial profits generated by selling access to data about transactions using the local currency are returned to citizens in the form of a dividend.

Viljoen's 2020 paper articulates the rationale for reorienting power relationships within the digital economy in favour of communities and to enable them to exercise meaningful control over their data⁴⁶. The paper argues that the process of data collection, use and sharing requires reworking on account of its social effects, whereby "personal choices over data sharing should reflect the effects this choice has on others, not only because of the political and moral benefits of considering others, but also because under current conditions of datafication".⁴⁷ It also builds on Elinor Ostrom's ground-breaking research on the governance of lakes, forests and other common pool resources, which demonstrates how communities can forge institutional frameworks to govern their use in a sustainable and mutually beneficial manner. The resultant theory of self-regulation by communities - termed Ostrom's design principles - holds invaluable insights for assigning collective rights over data.⁴⁸

Overall, bottom-up data stewardship represents an opportunity to subvert existing patterns of storing and sharing data⁴⁹, empowering groups to play an active role in deciding how and the purposes for which data can be used.⁵⁰

41 Driver's Seat Cooperative LCA (2021). Retrieved from <https://driversseat.co/>

42 Swashapp.io (2021). Retrieved from <https://swashapp.io/>

43 Open Humans Foundation (n.d.). Retrieved from <https://www.openhumans.org/>

44 MIDATA (n.d.). Retrieved from <https://www.midata.coop/en/home/>

45 Gyeonggi Do (2021), Gyeonggi Province Becomes First Local Autonomy in World to Implement a Data Dividend. Retrieved from: <https://english.gg.go.kr/blog/daily-news/gyeonggi-province-becomes-the-first-municipality-in-the-world-to-implement-a-data-dividend-governor-lee-jae-myung-says-it-is-the-beginning-sign-of-the-era-of-data-sovereignty/>

46 Viljoen, S., (2020) Yale Law Journal, Forthcoming. "Democratic Data: A Relational Theory For Data Governance", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3727562

47 Ibid

48 Coyle (2020), Ada Lovelace Institute, "Common governance of data: Appropriate models of collective and individual rights", <https://www.adalovelaceinstitute.org/blog/common-governance-of-data/>

49 Sundarajan (2020), Aapti Institute, "Role of data stewards in enhancing accountability", Role of data stewards in enhancing accountability

50 Manohar, Kapoor and Ramesh (2019), Aapti Institute, "Data stewardship: A Taxonomy", <https://thedataeconomylab.com/2020/06/24/data-stewardship-a-taxonomy/>

Data justice: A social justice agenda for the digital age

Growing datafication is a significant feature of contemporaneous capitalism, such that human and economic development have come to be governed by digital footprints that people leave in the wake of their interactions with technology. Consequently, the ways in which data is processed by corporations and governments affect not only the organisation of information, but also people's access to services and ultimately, their autonomy itself.

Scholars such as Linnet Taylor⁵¹ have drawn attention to the "structural discrimination" inherent to intensifying datafication, such that institutions of the state (through population databases and surveillance) and corporations (as dominant entities with accumulated data and processing abilities) function to amplify exclusion and disempowerment of individuals and communities. Elsewhere, Lina Dencik and Anne Kaun⁵² illustrate the debilitating impact of datafication on the welfare state, leaving citizens with limited bargaining power and agency to control the use of their data.

In such a milieu, reconstituting the conventional agenda of social justice becomes crucial to forge ethical pathways to regulate datafication. Data justice is an expression of this impulse, making "fairness in the way people are made visible, represented and treated as a result of their production of digital data" as crucial considerations that should guide policy and regulation on data.

1.3. Data trusts: an evolving conceptual framework

The concept of 'data trusts' has evolved from this backdrop of bottom-up data stewardship. The idea of extracting value from data and restructuring its distribution through the use of data trusts was posited by Professor Neil Lawrence in 2016,⁵³ whereby data trusts could act as "power brokers" to mediate the use of data for public benefit, without compromising the rights of data subjects to whom the data relates.

Subsequently, Delacroix and Lawrence articulated 'bottom-up data trusts' in 2019⁵⁴ as a tool of collective engagement used by communities to decide on how their data is used and shared by third parties. They described how trustees could be bound by fiduciary obligations of undivided loyalty and care towards its beneficiaries, defining the terms for purpose-led data sharing. It set out use cases to outline the advantages of the approach in different contexts. For example, in the context of social media and financial information, data trusts could have a role to play in negotiating terms on behalf of data subjects to ensure data could be made available for research and public policy purposes.

The Data Trusts Initiative builds on this conception of data trusts. It describes them as a "mechanism for individuals to pool their data rights into an organisation"⁵⁵, with i) independent stewardship of the pooled rights, ii) fiduciary responsibilities, iii) operations guided by a framework of institutional safeguards and iv) the facilitating of collective action.⁵⁶ This conception of the data trust seeks to rebalance the respective control that corporations and individuals have over personal data, and provide a legal mechanism to empower data subjects to choose to appoint others to make those decisions on their behalf. As a Mozilla

51 Taylor (2017), Sage Journals, "What is data justice? The case for connecting digital rights and freedoms globally", <https://journals.sagepub.com/doi/10.1177/2053951717736335>

52 Dencik and Kaun (2020), Global Perspectives - University of California Press, "Datafication and the Welfare State", <https://online.ucpress.edu/gp/article-abstract/1/1/12912/110743/Datafication-and-the-Welfare-State?redirectedFrom=fulltext>

53 Lawrence (2016), The Guardian, "Data trusts could allay our privacy fears", <https://www.theguardian.com/media-network/2016/jun/03/data-trusts-privacy-fears-feudalism-democracy>

54 Lawrence and Delacroix, International Data Privacy Law (2019), "Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance", <https://academic.oup.com/idpl/article/9/4/236/5579842>

55 Data Trusts Initiative (2021), "Data trusts: international perspectives on the development of data institutions",

<https://static1.squarespace.com/static/5e3b09f0b754a35dcb4111ce/t/603ce3325e1da817afe6b193/1614603061204/WP+2+-+DTI+-+global+perspectives.pdf>

56 Ibid.

Fellow, Anouk Ruhaak is also working on scenarios where multiple people ‘hand over their data assets or data rights to a trustee’, such as data donation platforms that allow users of web browsers to donate data on their usage of different services.⁵⁷

Similarly, Aapti’s interpretation of a data trust refers to “a legal arrangement wherein a person authorises an individual or entity to manage certain property for the benefit of a third party or for certain defined purposes”.⁵⁸ In the context of the data economy, the data (or rights over it) constitutes the property⁵⁹ that will be managed by the trust and the trustee (authorised representative individual or entity) is bound by fiduciary obligations to act in the best interests of its beneficiaries and according to the defined purposes.

Another major work outlining the potential function of data trusts is that of McDonald and Wylie⁶⁰. Their work describes the potential for data trusts in consumer protection and fiduciary governance for the data economy.⁶¹ It argues that the data trust, a legal arrangement where a trustee is appointed with fiduciary obligations towards a specified beneficiary, is suited to creating predictable data supply chains with increased accountability.

As a model of bottom-up data stewardship, data trusts represent a compelling instrument to unlock data for public benefit uses within a framework of fiduciary duties, such that data sharing decisions are compliant with the interests and rights of communities.⁶² As the Global Partnership for AI has itself described, they offer the potential to “expand access to data for innovation while putting citizen interests at the heart of stewardship”.⁶³

1.4. Differing interpretations of data trusts

There has been a lack of consistent, global interpretation of data trusts among scholars, policymakers and other actors, reflecting the nascent nature of the research and practice of bottom-up data stewardship.

India’s proposed framework for the governance of non-personal data recommends the appointment of data trustees as representatives to steward community data and channel its use for socially beneficial purposes such as entrepreneurship, innovation, research and policymaking.⁶⁴ Similarly, Ontario state authorities in Canada are exploring legal mechanisms to establish data trusts that would enable ‘privacy-protective data sharing’.⁶⁵

The European Commission’s proposed Data Governance Act, 2020 outlines a framework for “data intermediaries” - entities which provide “data sharing services” that “contribute to the efficient pooling of data as well as to the facilitation of bilateral data sharing”.⁶⁶ Although the Act does not explicitly identify a specific category or type of data intermediary, scholars have put forth data trusts as possible mechanisms to promote enfranchisement and meaningful realisation of data rights of subjects within the EU.⁶⁷

57 Ruhaak (2019), Mozilla Foundation, “Data trusts: Why, what and how”, <https://medium.com/@anoukruhaak/data-trusts-why-what-and-how-a8b53b53d34>

58 Manohar (2019), Aapti Institute, “Trust Law, Fiduciaries and Data Trusts”, https://thedataeconomylab.com/wp-content/uploads/2020/10/DataTrustsPpr_SM.pdf

59 Certain scholars have demonstrated that data lacks the requisite quality to be considered and treated as “property” in law. Refer Professor McFarlane’s work for more information - <https://www.law.ox.ac.uk/research-and-subject-groups/property-law/blog/2019/10/data-trusts-and-defining-property>

60 McDonald, S., Wylie, B. (2018), CIGI, “What is a Data Trust”, <https://www.cigionline.org/articles/what-data-trust/>

61 McDonald, S., Wylie, B. (2018), CIGI, “What is a Data Trust”, <https://www.cigionline.org/articles/what-data-trust/>

62 Sadowski, Vijjoen and Whittaker (2021), Nature, “Everyone should decide how their data is used - not just tech companies”, <https://media.nature.com/original/magazine-assets/d41586-021-01812-3/d41586-021-01812-3.pdf>

63 The GPAI Data Working Group (2021), “Understanding Data Trusts”, <https://ceimia.org/wp-content/uploads/2021/07/2021-07-09-GPAI-summary-understanding-data-trusts-updated.docx.pdf>

64 Kris Gopalakrishnan, et al., (2020), Ministry of Electronics and Information Technology (Govt. of India), “Report by the Committee of Experts on Non-personal Data Governance Framework”, https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf

65 Newsroom (2020), Government of Ontario, “Ontario Launches Consultations to Strengthen Privacy Protections of Personal Data”, <https://news.ontario.ca/en/release/57985/ontario-launches-consultations-to-strengthen-privacy-protections-of-personal-data>

66 European Commission (2020), “European Data Governance (Data Governance Act)”, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767>

67 Data Trusts Initiative (n.d.), “Understanding the Data Governance Act: In conversation with Sylvie Delacroix, Ben McFarlane and Paul Nemitz”, <https://datatrusts.uk/blogs/understanding-the-data-governance-act-in-conversation-with-sylvie-delacroix-ben-mcfarlane-and-paul-nemitz>

In the UK, a 2018 report by Hall and Pesenti called for the creation of data trusts as a “trusted and proven framework” to increase the availability and use of data for growing the domestic AI industry.⁶⁸ Other research subsequently interpreted data trusts as ‘providing independent fiduciary stewardship of data’, building on the work of Porcaro and others that had imagined organisations “[putting] their user-data in some form of irrevocable, spendthrift-esque ‘data trust’, which would then be managed by a third-party trustee (a nonprofit, for instance)”. Using this interpretation, the ODI undertook pilot projects to generate insights on the potential application of data trusts in the contexts of food waste management, wildlife poaching and urban mobility.⁶⁹ It has also observed UK Biobank, OpenCorporates and Oversight Board as examples of independent, fiduciary stewardship of data applied in practice⁷⁰.

This interpretation is adopted elsewhere. Based in the US, PLACE describes itself as a data trust for creating, storing and accessing mapping data, governed by independent trustees drawn from different geographies and sectors⁷¹. Johns Hopkins Medicine has similarly been described as having ‘a data trust administrator’, responsible for retaining patient privacy while enabling medical records to be used to improve care and facilitate research⁷². Toronto’s experience with a proposal to set up a ‘civic data trust’ is another example that worked to this interpretation.⁷³ In 2019, Sidewalk Labs proposed setting up a civic data trust to govern data generated by sensors and cameras around the neighbourhood that would be developed. Ultimately, the project was abandoned in 2020 citing unprecedented economic uncertainty but perhaps mostly due to local opposition to the development plans.

This research works to a definition based on the Global Partnership for AI’s consensus statement, whereby a data trust is “a form of data stewardship that supports data producers to pool their data (or data rights) with the aim of collectively negotiating terms of use with potential data users, through the oversight by independent trustees, with fiduciary duties, and within a framework of technical, legal and policy interventions that facilitate data use and provide strong safeguards against mis-use”. This interpretation is aligned with the concept as put forward by Lawrence and Delacroix in their paper on ‘bottom-up data trusts’ and as adopted by the Data Trusts Initiative. It marries the conception of groups of individuals coming together to contribute data within the framework of independent fiduciaries duties.

1.5. Institutionalising data trusts and codifying fiduciary responsibilities

There has been significant discussion around the challenge of institutionalising the data (or data rights) to be held and managed by data trusts, and codifying the fiduciary responsibilities of trustees.

Establishing data trusts involves the pooling of data, or data rights, and the exertion of control over these data (rights) by a trustee. Data rights enshrined within legislation are therefore a prerequisite for their development.⁷⁴ Over the past decade, we have seen the introduction of significant new data protection laws globally that represent the basis of a data rights framework. Jurisdictions in Canada have implemented data protection legislations at the federal⁷⁵ and provincial levels,⁷⁶ with Ghana close behind in enacting its Data Protection Act, 2012.⁷⁷ The most significant step towards articulation of data rights is the EU’s General Data Protection Regulation, 2016⁷⁸ which sought to impose controls on data processing, rooted in principles of individual harm, rights and privacy. This has spurred a flurry of personal data protection regulations that have

68 Hall and Pesenti (2017), “Growing the Artificial Intelligence Industry in the UK”,

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf

69 Open Data Institute (2019), “Data trusts: lessons from three pilots”, <https://theodi.org/article/odi-data-trusts-report/>

70 Hardinges (2020), The Open Data Institute, “Data trusts in 2020” <https://theodi.org/article/data-trusts-in-2020/>

71 Verhulst et al (n.d.), PLACE, “Establishing a data trust: From concept to Reality”, <https://www.thisisplace.org/blog-1/introducingplace/establishing-a-data-trust>

72 Dell Technologies (2019), “Lessons from a user-trusted data trust”, <https://www.delltechnologies.com/en-us/perspectives/lessons-from-a-user-trusted-data-trust/>

73 Tusikov (2019), Centre for Free Expression, ““Urban Data” and “Civic Data Trusts” in Smart Cities”, <https://cfe.ryerson.ca/blog/2019/08/%E2%80%9CUrban-data%E2%80%9D-%E2%80%9Ccivic-data-trusts%E2%80%9D-smart-city>

74 Data Trusts Initiative (2021), “Data trusts: international perspectives on the development of data institutions”,

<https://static1.squarespace.com/static/5e3b09f0b754a35dcb4111ce/t/603ce3325e1da817afe6b193/1614603061204/WP+2+-+DTI+-+global+perspectives.pdf>

75 The Personal Information Protection and Electronic Documents Act, 2004

76 To date, Alberta, British Columbia and Quebec have provincial laws to govern processing of personal information. Additionally, Ontario, Newfoundland and Labrador, Nova Scotia and New Brunswick have enacted independent legislations on health information processing.

77 The Data Protection Act, 2012 (Act 843)

78 Regulation (EU) 2016/679 - General Data Protection Regulation

been introduced or implemented in multiple jurisdictions outside Europe, such as India,⁷⁹ Kenya,⁸⁰ Brazil,⁸¹ South Africa,⁸² among others.

However, despite alignment between some regions, there remain significant variations in the data rights afforded by different jurisdictions. In addition to these variances, it is important to note that the manner in which specific rights - such as the right to data portability, which is crucial to support bottom-up data stewardship - are enforced differ across legal regimes. Further complications arise for jurisdictions that do not have an operative data protection legislation and consequently, provide little clarity on the data rights of citizens.⁸³ Therefore, the feasibility of data trusts will be a function of the extent and nature of data rights afforded by the relevant legal jurisdiction, and the way those rights are enforced. This dynamic is explored further in legal research undertaken by Aapti in parallel to the research described by this report.

Enabling data sharing for social benefit through data trusts: Legal review

In addition to the present research, Aapti was commissioned by GPAI to examine the existing and necessary legal mechanisms required to develop data trusts. To do so, the researchers undertook a rigorous process of comparative legal analysis across 11 jurisdictions to draw out variations in data protection laws and rights, data sharing frameworks and fiduciary obligations - all of which constitute essential legislative underpinnings of a data trust.

The resultant comparative analysis throws up several key insights that demonstrate disparity in maturity of legal landscapes for data trusts around the globe, and point to the need for administrative and legislative investments in data governance in several countries. Further, it was found that for legal systems which do not embed fiduciary duties matching common law structures, there may be a need to explore diverse structures for enabling human-centric data governance. Key takeaways from this research have been summarised below:

- **Disparity across nations and lack of digital infrastructure:** Given the diversity - both economic and political - of the jurisdictions analysed, it was found that the maturity in articulating rights over data varied significantly. This includes regulatory measures like standardisation of data formats or sharing purpose, enabling interoperability, or introducing digital public infrastructure.
- **Personal data rights and building for autonomy:** Even within some of the countries with more robust digital infrastructures, the absence of certain personal data rights - such as access, portability and erasure - pose challenges in creating a sustainable data trust ecosystem. For instance, Canada, Australia, and South Korea, while faring well on digital infrastructure, have yet to recognise clear data portability rights.
- **Legislative implementation and regulatory oversight:** Legal concepts which may be common across jurisdictions are not always implemented uniformly. For instance, the extent of adoption of trusts in Kenya and South Africa - countries with common law origins - is not as crystallised as compared to jurisdictions such as England, which extensively use trusts for a variety of commercial and non-commercial purposes.
- **A 'data trust conundrum' for stewardship:** It is evident that the conception of data trusts is most fundamentally rooted in English trust law. Based on this analysis, even in jurisdictions that have common law influence and recognise trusts, the evolution of its concepts have not mirrored the English experience.

79 The Personal Data Protection Bill, 2019

80 The Data Protection Act, 2019

81 Lei Geral de Proteção de Dados, 2019

82 Protection of Personal Information Act, 2013 (came into force, partly, in 2020)

83 For more information on the status of data protection and privacy legislations across the world, refer to the UNCTAD's remarkable tracker available at <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

In the past, the role of fiduciaries in the context of data stewardship has generally been limited to ensuring compliance - that is determining whether grounds for processing of data are in accordance with applicable regulations.⁸⁴ However, this conception of 'trustees' holding broader and more explicit fiduciary duties that compel them to act in the best interests of data producers has started to be discussed within the data governance ecosystem. This renewed approach to the duties of "trustees" has its roots in the stewardship of common pool resources, such as Scotland's ports trusts.⁸⁵ With myriad activities - from fisheries management to renewable energy generation - being undertaken, the ports are managed through a trust framework set through an act of law of the Parliament. These trust ports are governed by a stakeholder-representative board comprising users of the port, members of the local community, government agencies and follows a democratic model of decision-making. The trust framework helps balance various perspectives and interests while generating valuable income for regional and national economies; at the heart of the trust port model is the fiduciary duty of loyalty and care which mandates trustees to act in the best interest of its stakeholders.⁸⁶

Sean McDonald⁸⁷ has expanded on the application of explicit, contextual fiduciary duties to the governance of data, describing data trusts as a tool to hold companies accountable for their decisions and the promises made to users. In this view, data trusts offer a credible legal container for articulating fiduciary accountability and establishing processes to enable the right of redress.

The concept of information fiduciaries⁸⁸ proposed by Balkin also provides a seminal analysis of fiduciary duties. It has, however, been subject to criticism,⁸⁹ chiefly in that the approach fails to take cognisance of the entrenched business models that drive diverging interests between end users and data processors. According to this criticism, users are not adequately equipped by platforms and data processors in order to express and act on their interests, which is not changed by the imposition of fiduciary duties on data processors. Also, as fiduciary obligations are normally settled by courts, the cost of solving each dispute on violation of fiduciary obligations may prove to be too much for users as well as the legal system to bear.⁹⁰

Divergent views have also been expressed as to the legal forms most suitable for data trusts to take to 'house' the data (rights) contributed by data subjects, and to codify the fiduciary responsibilities of its trustees.

In the UK, the ODI worked with a legal consortium on its initial pilots who argued that the mechanism of trust law was 'inappropriate' for constructing data trusts, largely on the basis that data cannot be made the property of a trust under existing law⁹¹. This statement was subsequently challenged by the legal community. In October 2019, Professor Ben McFarlane of University of Oxford questioned this finding, suggesting that people's rights over data, such as those conferred by the General Data Protection Regulation, rather than data itself, could be made the property of a legal trust and asserted collectively by its trustees.⁹² A similar argument has been made by Sylvie Delacroix and Neil Lawrence, who have suggested that while there are challenges, they 'do not constitute reasons to doubt that data rights can be held under a legal Trust'. A paper published in the National University of Singapore Faculty of Law's journal similarly found that 'the traditional trust, the historical creation of English Equity jurisprudence and now found around the world, is a perfectly sensible vehicle for the management of data'.⁹³

84 Bailey and Goyal (2019), Data Governance Network, "Fiduciary relationships as a means to protect privacy: Examining the use of the fiduciary concept in the draft Personal Data Protection Bill, 2018", https://datagovernance.org/files/research/NIPFP_Rishab_Trishree_fiduciaries_-_Paper_4.pdf

85 Transport Scotland (n.d.). Retrieved from <https://www.transport.gov.scot/transport-network/ports-and-harbours/port-governance/>

86 Kapoor and Ramesh (2019), The Data Economy Lab, "Principles for Revenue Models for Data stewardship", <https://thedataeconomylab.com/2020/07/31/principles-for-revenue-models-of-data-stewardship/>

87 McDonald, S. (2019), The Fiduciary Supply Chain: Models for Platform Governance, <https://www.cigionline.org/articles/fiduciary-supply-chain/>

88 Balkin, J. (2016), UC Davis Law Review, Vol 49, No.4, "Information Fiduciaries and the First Amendment", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3700087

89 Pozen, D. and Khan, L. (2019) "A Skeptical View of Information Fiduciaries", Harvard Law Review, 2019, <https://harvardlawreview.org/2019/12/a-skeptical-view-of-information-fiduciaries/>

90 Ibid

91 Open Data Institute (2019), "Data trusts: lessons from three pilots", <https://docs.google.com/document/d/118RqyUAWP3WlyyCO4iLUT3oOobnYJGibEhspr2v87jg/edit>

92 McFarlane (2019), University of Oxford - Faculty of Law, "Data trusts and defining property", <https://www.law.ox.ac.uk/research-and-subject-groups/property-law/blog/2019/10/data-trusts-and-defining-property>

93 Lu Jia Jun, et.al. (2019), NUS Law Working Paper No. 2019/019, "The basics of private and public data trusts", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3458192##

The use of alternate legal forms to construct data trusts may be appropriate in jurisdictions that do not follow the common law tradition. For example, Germany does not have a trust law framework, but nonetheless has institutional forms such as the Sparkassen (cooperative or not-for-profit banks) that carry fiduciary obligations ascribed to the common law trust. And in Quebec, a civil law jurisdiction, the Quebec trust enables data rights to be pooled and administered by a trustee, which has sparked widespread excitement around the opportunity.⁹⁴ These examples indicate the difference in legal structures being experimented with in different legal jurisdictions in order to facilitate the development of data trusts.

94 Hulin (2021), Data Trusts Initiative, "How can civil law jurisdictions support data trusts? The Quebec example", <https://datatrusts.uk/blogs/how-can-civil-law-jurisdictions-support-data-trusts-the-quebec-example>

2. International knowledge, attitudes and practices of data trusts

- This section describes the results of a survey to understand knowledge (awareness and understanding), attitudes (perspective) and practices (implementation) of data trusts around the world.
- Respondents included those operating data trusts or similar bottom-up data stewardship initiatives, and organisations working on the topic of data stewardship.
- The survey: surfaced awareness of and optimism towards the concept of data trusts; found general agreement with the definition put forward by GPAI; found no projects delivering all the functions of real-world data trusts through one vehicle but a number of similar bottom-up data stewardship initiatives that were delivering many of the functions; and encountered a variety of legal forms and technologies used to construct the different initiatives.

2.1. Context

This section describes the results of a survey undertaken to understand the knowledge about, attitudes towards and practices of data trusts from around the world.

The survey was divided into four sections. The first covered basic information about the respondent: their country of work, role and organisation name. The second sought their current understanding of data trusts, and included questions about the definition of data trusts and other forms of data stewardship. The survey then split into two parts, with one for completion by practitioners (people building or running data trusts, or similar bottom-up data stewardship initiatives) and the other for experts working on data stewardship and related topics. Practitioners were asked questions about how their initiatives work and whether they identified themselves as data trusts. Experts were asked about their perceptions of the current state of data trusts, and their thoughts about the future of the movement. In general, the survey combined structured and open-ended questions designed to enable quantitative analysis as well as space for respondents to elaborate their ideas.

The survey was initially distributed by Aapti and ODI to around 100 practitioners and experts. It was also disseminated through social media platforms and newsletters, the GPAI Working Group, and snowballed through respondents sharing the survey themselves. At the close of the survey there were 45 responses. There was an even split between practitioners and experts, 22 and 23 respectively. Responses were heavily-weighted towards Europe (and in particular from the UK), with nearly $\frac{3}{4}$ of all the respondents working there. The sectors that respondents described working from were technology and data, health and research.

2.2. Awareness and understanding

The concept of data stewardship was a familiar topic for the respondents of the survey, as you might expect from practitioners and experts. Respondents were slightly less familiar with the idea of data trusts.

Familiarity with data stewardship and data trusts

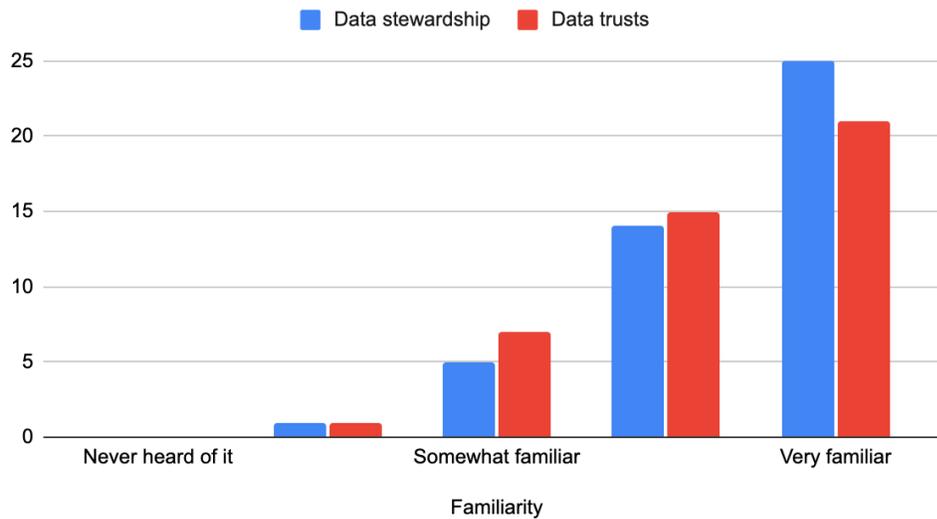


Figure 1: Respondents familiarity with data stewardship and data trusts

Beyond data trusts, our respondents were aware of a variety of other forms of data stewardship - the most familiar being data trusts, data commons, and data exchanges. The familiarity with data trusts was unsurprising given the focus of this project. Respondents also shared examples of data stewardship that were not listed as prompts, such as statistics agencies and national bodies.

As the literature review details, there are varying interpretations of data trusts. In this case, 82% of respondents agreed with the GPAI definition of data trusts as “a form of data stewardship that allow data producers to pool their data (or data rights) and facilitate collective negotiation of terms of use with potential data users, working through independent trustees who are bound by strong fiduciary duties, within a framework of technical, legal and policy interventions that facilitate data use and provide strong safeguards against mis-use”. The respondents who did not agree with the definition offered a variety of interesting ideas and opinions.

A number of respondents disagreed with the language used in the GPAI definition. In one case, the respondent felt that the who the trustees have a fiduciary duty to was missing, preferring the language of trustees “*acting on behalf of the data subjects*”. The respondent also described the need for data trusts to be working towards a specific purpose and felt this should be reflected in the definition. Other respondents questioned the use of the term “*data producer*” and requested that the legal mechanism intended to create the fiduciary duties should be documented.

A further contention made by respondents was whether the definition reflected a feasible reality. In particular, respondents questioned whether the imposition of fiduciary duties and technical, legal and policy safeguards was an ideal, and too high a bar to be met. One respondent preferred to talk about ‘data intermediaries’ and another described there not to be a need for an independent trustee. These responses perhaps represent something deeper than varying ideas for the definition of data trusts, and instead reflecting the existence and need for various forms of bottom-up data stewardship.

When asked to list examples of data trusts, respondents responded in three ways:

- They gave examples of similar bottom-up data stewardship initiatives (the difference between these and data trusts is discussed below).
- They gave theoretical examples of data trusts.
- They stated that they were not aware of any practical examples of data trusts.

A number of examples given by respondents - including Swash⁹⁵ and MIDATA⁹⁶ - did not appear to have all of the functions of a data trust set out by the GPAI definition. In particular, none appeared to have independent trustees with fiduciary responsibilities. Other examples were not yet active, like the Liverpool Civic Data Cooperative⁹⁷. Other examples were theoretical or abstract, such as 'a Health Bank', a theoretical data trust of residents of a housing block and mentions of the examples put forward by Sylvie Delacroix and Neil Lawrence's paper⁹⁸.

2.3. Practices

To find out about the practices of data trusts, part of the survey was targeted specifically to practitioners who are building or running data trusts.

These questions focused on understanding how each initiative identified itself, their function and purpose, and included practical questions on their approach to data stewardship. There were 22 respondents to this part of the survey.

In terms of identifying their initiatives, around a third of practitioners did not identify as data trusts. Within these respondents, we observed two main types of organisations. The first consist of organisations like Schluss & digi.me, who see themselves as the creators of infrastructure onto which data trusts can be built - for example by creating the technology for users to collect their data in a pod or vault. The second was formed of organisations with similar aims to the concept of data trusts, as put forward by GPAI, but function differently. For example, Swash described having "built-in trustless structures" rather than fiduciary responsibilities to achieve the outcome of empowering people with their data, and CSIRO detailed how they work to enable the aggregation of data for the common good but unlike data trusts, participating actors control what happens to the data rather than trustees.

The survey asked practitioners to select which of the 6 functions, as per the GPAI definition of data trusts, their initiatives undertake, as follows:

1. Provide a platform for people to pool data.
2. Provide a platform for people to establish desirable terms and conditions of data use.
3. Negotiate use of the data in accordance with agreed terms and conditions, facilitating safe and controlled data use.
4. Appoint expert trustees to take responsibility for the stewardship of the data.
5. Create a regime of strong fiduciary responsibilities to bind the trustees to act in the interests of the data trust's members.

95 Swash, (2021). Retrieved from: <https://swashapp.io/>

96 MIDATA, (2021). Retrieved from: <https://www.midata.coop/en/home/>

97 Liverpool Civic Data Cooperative, (2020). Retrieved from: <https://www.liverpoolcityregion-ca.gov.uk/liverpool-city-region-combined-authority-announces-proposals-for-5-3m-funding-for-data-driven-health-improvements/>

98 Lawrence, N. & Delacroix, S. (2019, October 1). Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance. International Data Privacy Law. Retrieved October 26, 2021, from <https://academic.oup.com/idpl/article/9/4/236/5579842>.

6. Establish safeguards and oversight mechanisms to prevent data misuse and to take remedial action in the event of the trust's terms and conditions being breached.

On average, the respondents stated that they had between four and five of the functions, with responses ranging from just one to the full six.

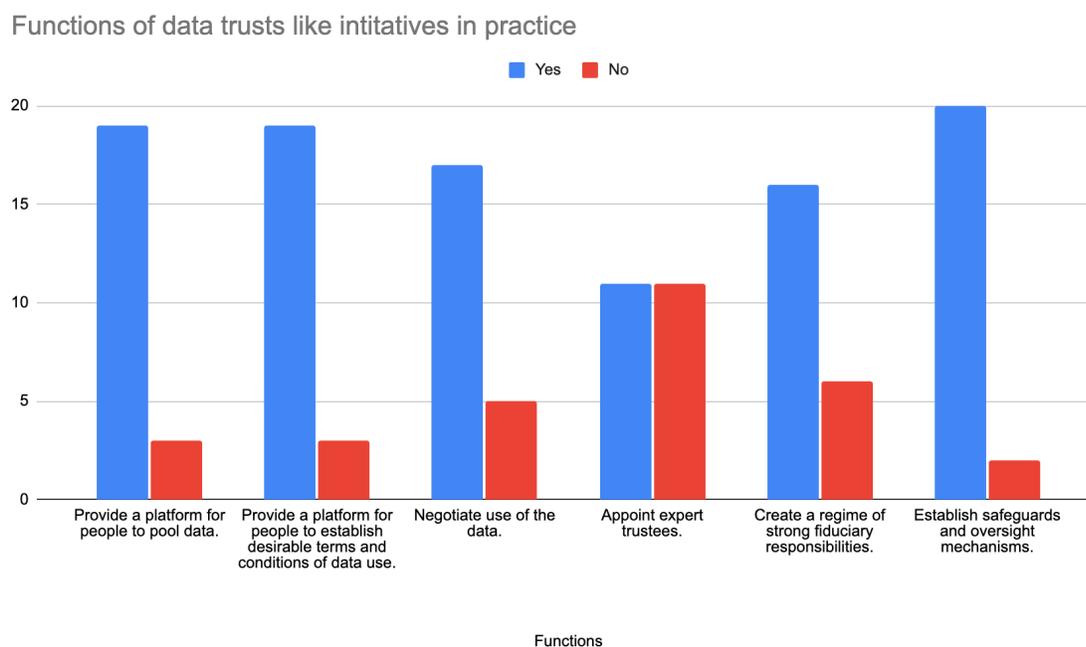


Figure 2: “Which of the following functions does your initiatives have?” - question to data stewardship practitioners.

There was a relatively even distribution across five of the six roles, with one function outlying: *Appoint expert trustees to take responsibility for the stewardship of the data*. This may reflect that the requirement to appoint expert trustees to oversee the stewardship of data may be one of the more difficult functions to achieve in practice. Conversely, providing a platform to pool data, and establishing safeguards over that data, appear some of the more common and achievable functions in practice.

Seven respondents said their initiatives had all six of these functions, appearing to determine them as data trusts. However, of these seven: the name of one of these was not given (N/A); two were not yet active (PLACE, Donate your Data Foundation); two instead develop technology for data trusts (Sightline Innovation, PolyPoly); and one preferred not to define as a data trust (DataYogi). This left one for us to examine further (Worker Info Exchange).

Worker Info Exchange is a non profit organisation dedicated to helping workers access and gain insight from data collected from them at work.⁹⁹ The project is relatively early stage, but is active and currently stewards data on behalf of gig workers. On their website, there is clear evidence they are providing a platform to pool data and establish desirable terms, they are negotiating safe usage of their users data, and establishing safeguards to prevent data misuse. However, it is unclear as to whether there are any data trustees and whether those trustees have fiduciary responsibilities to act in the best interests of their members. The lack of evidence means that for the purposes of this report, Worker Info Exchange is not considered a data trust.

⁹⁹ Worker Info Exchange, (2021). Retrieved from: <https://www.workerinfoexchange.org/>

Despite not meeting the GPAI definition, Worker Info Exchange is an excellent example of bottom-up data stewardship in practice¹⁰⁰.

The survey also asked experts about the frequency that they had seen the six functions of data trusts in their work.

Frequency of functions of data trusts as seen by experts

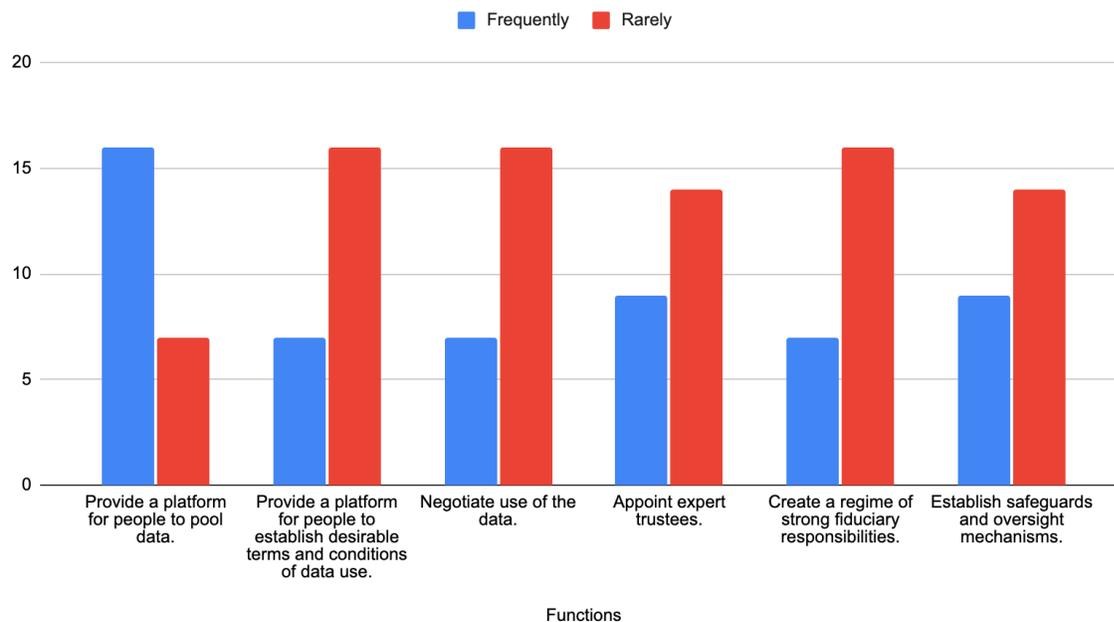


Figure 3: “In the data stewardship initiatives you have come across in your work, please select the frequency that you see the following features” - question to data stewardship experts.

Two thirds of the experts had frequently seen initiatives *providing a platform for individuals and groups to pool their data*. The other 5 functions were rarely observed in a practical setting.

The survey explored how bottom-up data stewardship initiatives function, asking respondents to describe legal forms, technical systems and business models.

Data trusts have been conceptualised as being constructed using trust or common law, but only one respondent specified that they had given thought to this (they had undertaken some research to understand how trust law could be applied in their context). Respondents described a wide range of legal approaches used to underpin their initiatives. Limited companies, foundations and nonprofits were the most frequent legal forms, with constructs such as cooperatives also mentioned. A number of respondents alluded to the fact that different legal forms were suitable in different circumstances.

As well as the legal form of their initiative, respondents also commented on the wider legal conditions around them. Respondents cited the General Data Protection Regulation as a legislation or law that has been ‘specifically helpful or harmful to your initiative’. Other similar laws, such as the CDPR in California and the “Law for a digital republic in France” were also mentioned.

100 This project reached out to Worker Info Exchange to respond to this analysis, Worker Info Exchange agreed with our description of the initiative not currently meeting the GPAI definition, but described how the team was currently exploring whether becoming a data trust of this nature was a feasible undertaking.

The technologies adopted by the respondents were also varied. Some organisations described using blockchain, while the development of 'pods' or 'vaults' for personal data were also described. Blockchain was described as being useful by initiatives working towards creating a 'trustless' structure, in which the distributed technology was seen as replacing the need for trustees to make decisions. The 'pods' and 'vaults' were described by initiatives seeking to help users to have more control over data about them on an individual, rather than group, basis. There was also discussion of privacy enhancing technologies to ensure the safety of users' data, as well as Application Programming Interfaces to facilitate access to the data being brought together by the initiatives.

Respondents also shared information about their business models. Most of the respondents described being funded by non-earned revenue streams, such as philanthropic funding, public funding or private investment. The predominance of unearned revenue reflects the relative infancy of bottom-up data stewardship initiatives and finding them early in their quest for sustainability¹⁰¹. A quarter of respondents described earned revenue streams, including membership fees for the users of the initiative, selling access to data to third parties and analysing and packaging the data into insights.

In terms of the scale and maturity of the initiatives, 50% of the respondents had 1,000 members or less, and 80% of the initiatives are less than 5 years old (or are yet to be operational).

2.4. Attitudes towards data trusts

The survey also sought to understand the respondents' attitudes and perspectives on data trusts.

A number of survey respondents, both experts and practitioners, were positive about the potential of data trusts. By increasing the control people have over data about them, a number of respondents thought that data trusts could help to rebalance the power asymmetry in the data economy. One respondent stated that through data trusts, people's data could be better safeguarded from private interests, avoiding 'abusive data relationships'. Respondents felt data trusts could also work towards a future where there was increased access to and usage of data for public benefit. They described how data trusts could be designed to tackle "problems in which individuals are interested in combining their data to get a broader analysis of a specific challenge, or where individuals benefit from pooling their data".

Some respondents described the lack of practical examples of data trusts holding the concept back. There was a strong desire, verging on impatience, among some of the experts to see an operational data trust, even to the point where some described that the concept had become 'somewhat of a fantasy'. Others were concerned that the focus on an approach to bottom-up data stewardship that only exists as a concept may detract from other similar - but importantly, operational - approaches (such as those featured as case studies in this report). Some respondents were also concerned about the potential uptake of data trusts as and when they became functional, feeling that the demand for them originates largely from experts and reaching a critical mass of users would require a dramatic shift in culture, understanding and skills across the data economy.

101 Dodds, L., Szász, D., Keller, J., Snaith, B. and Duarte, S. (2020, April). Designing sustainable data institutions. Open Data Institute. Retrieved 26 October 2021, from: <https://theodi.org/article/designing-sustainable-data-institutions-paper/>.

3. Case studies

- This section consists of three case studies of bottom-up data stewardship initiatives: Driver's Seat, Open Humans and MIDATA.
- They represent real-world examples of how groups can be empowered around data they've generated, and are actively making available data for broad societal benefit.
- They have been selected on the basis of their community-centrism and maturity, and the studies unpack the purposes for their formation, their stakeholders served, their legal structure, their internal data governance principles and the technical safeguards used to mediate access to data.

3.1. Criteria and selection

This section of the report consists of three case studies of bottom-up data stewardship initiatives. They are intended to shed light on the practical considerations involved in designing such an initiative, and to surface perspectives from practitioners operating them.

The case studies rely on secondary research in the form of Aapti and the ODI's internal interview notes, analysis and videos. The cases were selected using the two criteria:

1. **Maturity** - There are many interesting proposals and theoretical models for data trusts and bottom-up data stewardship initiatives. However, for the purposes of the case studies, we skewed towards those that are operational (i.e. actively supporting data to 'flow' between actors).
2. **Community-centrism** - Empowering people to exercise meaningful control over data takes many forms. We have chosen cases that adopt a collective, participatory approach to data stewardship, such that their members dictate how their data is used, by whom and for what purposes.

Ideally, Aapti and the ODI would have liked to feature initiatives that responded to the survey as case studies. However, the researchers found that [Driver's Seat](#), [Open Humans](#) and [MIDATA](#) not just satisfy the above mentioned criteria more so than respondents, but are perhaps some of the most promising examples of bottom-up data stewardship in general.

As well as showing the variety of design choices available, the case studies, albeit anecdotal, highlight the virtues of bottom-up stewardship.

Aspect of analysis	 Driver's Seat	 OPEN HUMANS	 MIDATA
Purpose	Empower gig workers to take control of their data and derive monetary value through it	Facilitate community data governance to produce open, participant-centric research in health	Enable members to gain control over data and amass health data for use in biomedical research
Structure	Limited cooperative association; funded by pvt investments, grant money; revenue from monetization of aggregated insights	Non-profit organization; funded and sustained through grant money; does not generate any revenue	Non-profit cooperative; private investments and grant money source of funding; does not generate any revenue
Stakeholders	Gig workers are the data generators; data users include local government and transportation agencies	Individual members of OH comprise data generators; academic institutions, independent researchers are data users	Members and MIDATA account holders are data generators; pharmaceutical companies and research orgs. are data users
Governance principles	Data sharing and selling decisions governed through cooperative board; members can revoke consent for data use through email notices	Data sharing decisions are authorized by individuals and varies on a project-to-project basis	Data sharing authorized through internal ethics review board and general assembly of members through democratic votes
Privacy controls	Member data is anonymized, and only aggregated datasets and insights sold to data users/buyers	Data may or may not be anonymized/pseudonymized before sharing, varies according to project requirements	Data may or may not be anonymized/pseudonymized before sharing, varies according to project requirements

Figure 4: Snapshot of insights from case studies (Source: Aapti/ODI analysis)

3.2 Driver's Seat

Overview

Driver's Seat enables workers in the gig economy to gain control over their data and access analytics that help them earn more from their labour.

Founded in 2019 in Colorado, USA, the platform was developed over conversations with Uber and Lyft drivers whose work was mediated by the 'extraction, processing and delivering of data' via algorithms that tended to deny workers of their agency and a voice in negotiating their working conditions.¹⁰² Driver's Seat also aids in the monetisation of driver's mobility data by selling access to public authorities and local governments that use these insights in policy making and resource allocation.¹⁰³ Consequently, the entity unlocks societal value by directing data use towards public benefit, while simultaneously compensating the members of its cooperative for their role in generating this data.

102 Witt, Hays [Aapti Institute] (2021). "Data Economy Lab | Tracking Stewardship: Driver's Seat - Empowering gig workers through data" [Video]. Youtube. <https://youtu.be/a-l8tfeoB3g>

103 Ibid.

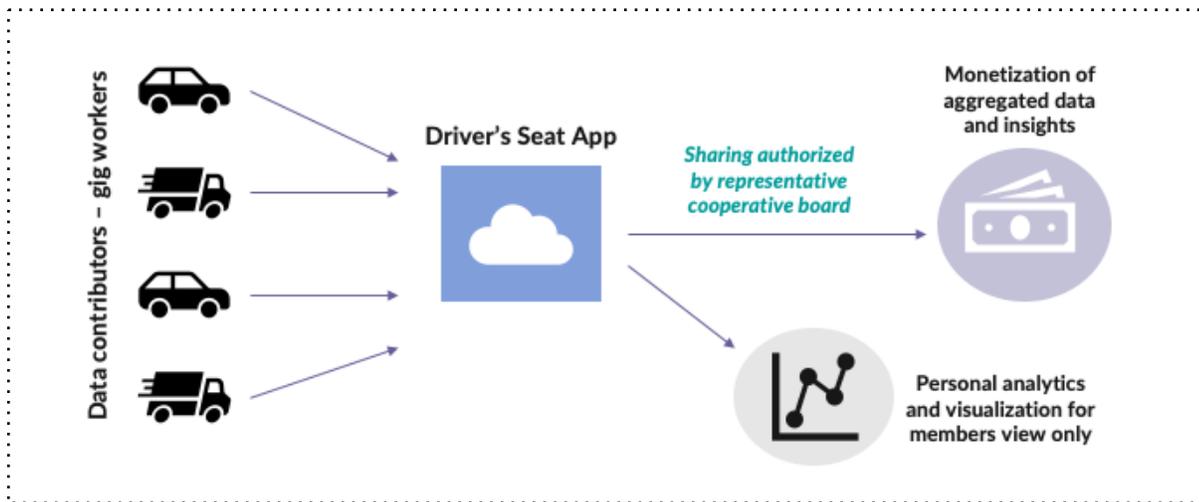


Figure 5: Structure of Driver's Seat (Source: Aapti/ODI analysis)

Purpose

The core stated purpose of Driver's Seat is to enable participation of gig workers in the governance of their data and derive monetary/instrumental value that could potentially reduce the precarity associated with platform-mediated labour. Additionally, the platform presents opportunities for monetisation of aggregated mobility data and its insights by selling it to public transportation agencies.¹⁰⁴ This information provides crucial inputs for policy making in areas such as pollution control and congestion management. In fact, municipal authorities are afforded visibility into rideshare operational patterns and analytics that are otherwise challenging to access or comprehend.

Structure

Driver's Seat is registered as a for-profit, limited cooperative association in Colorado, USA. The primary beneficiaries of this platform are rideshare and delivery workers who have signed up to become members of the cooperative. It adopts a delegated cooperative structure that is governed by a representative board, with at least 51% of the board members drawn from the larger community of workers.¹⁰⁵ This structure is quite unlike MIDATA, considered below, which instead adopts a 'one member, one vote', approach to internal governance.

Rideshare and delivery workers who are a part of Driver's Seat share data with the application, which functions as a data storage and analytics platform. Insights and visualisations created on the platform not only enhance the agency of gig workers by placing data in their control, but also provide crucial information that enables them to optimise for higher wages and better working conditions. Moreover, Driver's Seat enables this data to be shared with local government transit operators, promising to improve the reach and effectiveness of citizen service delivery and experience.¹⁰⁶

Membership fee, grant money and private investments are the intended funding streams for Driver's Seat. However, monetisation of insights and aggregated data sold to public authorities is currently its sole source of revenue.¹⁰⁷

¹⁰⁴ Dickey (2020), TechCrunch, "Coop helps Uber, Lyft drivers to use data to maximise earnings", <https://techcrunch.com/2020/02/06/co-op-helps-uber-lyft-drivers-use-data-to-maximize-earnings/>

¹⁰⁵ Stewardship Navigator (2021), Aapti Institute, <https://thedataeconomylab.com/> (pending publication)

¹⁰⁶ Ibid.

¹⁰⁷ Ibid.

Stakeholders

The primary stakeholders served by Driver's Seat are gig workers: rideshare and delivery drivers employed by Uber, Lyft, DoorDash, Uber Eats, Amazon Flex and Postmates operating within the US. These workers also constitute the data generators whose mobility information and personal data is managed by the platform.

Data users include local government and transportation agencies that use analytics and aggregated mobility data supplied by Driver's Seat as a part of urban policy and planning.¹⁰⁸

The representative board governing the cooperative is the designated decision-making body that authorises all data sharing and selling activities.

Governance principles

The data stewarded by Driver's Seat includes members' personal data as well as anonymised mobility information. The data rights are vested in the cooperative board, with individual members retaining only the right to revoke consent for data use.

Significantly, data sharing and selling decisions are authorised through the cooperative board in which gig workers hold at least 51% representation and voting rights. Further, the members are also entitled to a minimum 51% of the share of profits generated by Driver's Seat. The twin features of representation and share in profits are mandated by the Colorado Uniform Limited Cooperative Association Act, 2012.¹⁰⁹

Members of the cooperative participate in data decisions by electing representatives to the board. Individual consent for data access, processing and sharing is obtained at the point of on-boarding to the Driver's Seat application. Lastly, members can revoke consent for any of these functions and request deletion of their data via email.¹¹⁰

Privacy controls

Driver's Seat anonymises the data contributed by drivers and shares only aggregated datasets and insights with its data users once approved by the board.¹¹¹ Personalised analytics and visualisation derived from individual members' data is not shared with third parties.

Analysis

Monetisation of aggregated data and insights by Driver's Seat performs two functions - one, it contributes to the income of gig workers who are profit-participants in the entity and two, creates a viable source of revenue that contributes to the financial sustainability of Driver's Seat. Delegated representation afforded through the entity's cooperative board upholds participation of data generators in decision-making as a core of its operating principles.

The experience of Driver's Seat holds interesting insights for data trusts and data trust-like initiatives that hope to facilitate effective purpose-driven data sharing. Additionally, the social value element can be fulfilled by identifying appropriate stakeholders, in this case public transit agencies, who stand to benefit from the use of the data stewarded by the initiative. Delegated representation and decision-making through the cooperative board could potentially reduce the burden on beneficiaries to evaluate granular considerations on data sharing, while simultaneously availing valuable advisory services from the board.

108 Witt, Hays [Aapti Institute] (2021). "Data Economy Lab | Tracking Stewardship: Driver's Seat - Empowering gig workers through data" [Video]. Youtube. <https://youtu.be/a-l8tfeoB3g>

109 To better understand limited cooperative associations, visit https://www.sos.state.co.us/pubs/business/news/2012/20120402_ULCAA_Dean.html

110 Stewardship Navigator (2021), Aapti Institute, <https://thedataeconomylab.com/> (pending publication)

111 Ibid.

3.3. Open Humans

Overview

Open Humans is a not-for-profit that allows individuals and communities to donate personal data for use in research, education and health projects.

Established in 2015 in the US, the platform helps individuals access and understand their personal data through an Open Humans account and donate it for projects that align with their values or goals. The entity facilitates public benefit data sharing while providing granular and dynamic controls, creating opportunities for bottom-up decision-making and data governance.

Open Humans differs from Driver's Seat on two fronts: Open Humans supports granular decision-making functions by allowing each member to approve or disapprove use of their data in a specific project, and the incentive to participate is altruistic as the entity does not stand to make any profits or generate revenue from its sharing activities.



Figure 6: Structure of Open Humans (Source: Open Humans website)

Purpose

Open Humans is designed to empower individuals and communities around their personal information, by combining technology and community governance of data to advance an open, participant-centric approach to human subjects research.¹¹² It has built a platform for collaboration between communities and researchers, directing data to projects or purposes that fulfill the data donors' personal expectations. The entity also facilitates citizen science and subject participation in health research. Open Humans currently has 12,364 members.¹¹³

112 Ball, Mad [Aapti Institute] (2021). "Data Economy Lab | Tracking stewardship: Open Humans - Empowering citizens, patients and researchers through data" [Video]. Youtube. <https://youtu.be/L9GHP-u0gK4>

113 As on 20 September, 2021, reported on the organisation's website.

Structure

Open Humans is registered as a 501(c)(3) nonprofit organization in the US¹¹⁴. In addition to providing a platform for collaboration and data sharing, Open Humans allows individuals to run analytics on their personal data and understand it through free and open source “notebooks” that can be embedded in one’s browser.¹¹⁵ The entity is funded through grants from Robert Wood Johnson Foundation, Knight Foundation and Shuttleworth Foundation.¹¹⁶

Stakeholders

Individuals who have signed up as members of the Open Humans community are the data producers, while academic institutions, citizen scientists and researchers comprise the data requestors and users. Data sharing decisions are made by individuals who can agree to sharing their personal data, particularly health data, for a specific project. Therefore, consent is specific to a project and can be revoked at any point.¹¹⁷

Governance principles

The members of Open Humans are the primary decision-makers. They retain full control over their personal data and authorise its use through granular controls on a project-to-project basis.¹¹⁸ Individuals and communities willing to donate their data for research are encouraged to examine the purpose and value of a particular project before agreeing to share their data.

Similarly, any member of Open Humans - irrespective of their academic background - can create projects/research studies about a specific theme. This is best demonstrated through the many citizen science projects hosted on the platform.¹¹⁹ All projects undergo a community review process, performing a role akin to the ethics or internal review board within academia. The review is an open and public process in which every member can participate. Communities can de-platform a project as a part of the review process.¹²⁰

Privacy controls

Data may or may not be anonymised or pseudonymised before it is shared; it is dependent on the nature of research involved.¹²¹ Member data is centrally stored on the Open Humans platform and a copy in shareable formats is made available to third parties who have been authorized to access the data.¹²² Analytics, insights and visualisation accessed by individuals through personalised “notebooks” and such tools hosted on the platform are not shared with third parties, unless otherwise consented to by an individual.

Analysis

Open Humans presents a unique use case of a bottom-up data steward that is explicitly concerned with facilitating data sharing for social benefit. Individuals and communities are invited to become a part of the entity and participate actively in research projects that appeal to them personally, exploring themes that are otherwise often marginalised within conventional academic discourse. For instance, a project on the dynamics and perceptions of the neovagina is currently being hosted on the Open Humans platform. It allows members to deliberate on the research methodology and frame questions that should be addressed as a part of this study. In essence, the platform embeds health research within a strong framework of citizen-driven science and community interests.

114 Open Humans Foundation (n.d.). Retrieved from <http://openhumansfoundation.org/>

115 Ball, Mad [Aapti Institute] (2021). “Data Economy Lab | Tracking stewardship: Open Humans - Empowering citizens, patients and researchers through data” [Video]. Youtube. <https://youtu.be/L9GHP-u0gK4>

116 As disclosed in the organisation’s website on 20 September, 2021.

117 Stewardship Navigator (2021), Aapti Institute, <https://thedataeconomylab.com/> (pending publication)

118 Ibid.

119 Ball, Mad [Aapti Institute] (2021). “Data Economy Lab | Tracking stewardship: Open Humans - Empowering citizens, patients and researchers through data” [Video]. Youtube. <https://youtu.be/L9GHP-u0gK4>

120 Ibid.

121 Stewardship Navigator (2021), Aapti Institute, <https://thedataeconomylab.com/> (pending publication)

122 Ibid.

3.4. MIDATA

Overview

MIDATA is a member-owned cooperative that provides an open source technical platform for account holders to store their personal data and share it with researchers and service providers.

Developed by ETH Zurich and Bern University of Applied Sciences, MIDATA Switzerland was established in 2015 and the entity supports the creation of other regional or national cooperatives that use MIDATA's technical infrastructure.¹²³ MIDATA account holders can control who has access to their data and direct its use in specific clinical studies.

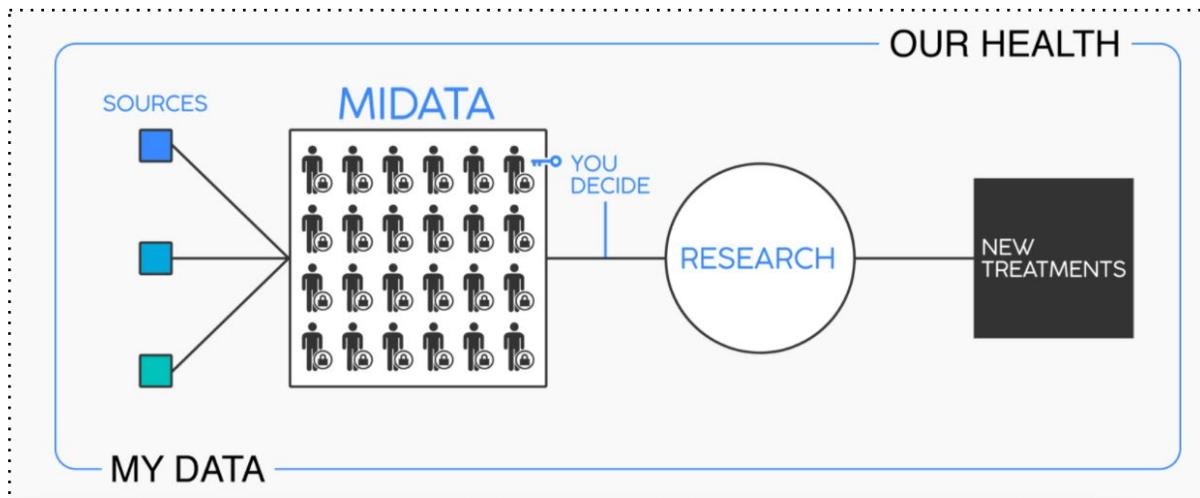


Figure 7: Structure of MIDATA (Source: MidData website)

Purpose

The cooperative was established to fulfill two objectives: to enable citizens to gain control over health information and to amass valuable aggregated health data for use in medical research.¹²⁴ MIDATA allows individuals to engage with health research projects and determine if they wish to contribute their data to a certain study. Thus, it facilitates active participation of data subjects in medical research.¹²⁵

Structure

MIDATA is a non-profit cooperative, registered under Article 828 of the Swiss Code of Obligations.¹²⁶ Its primary function includes the development, deployment and maintenance of a common technical infrastructure that allows MIDATA data account holders and members to store their personal data.

¹²³ Ibid.

¹²⁴ Ibid.

¹²⁵ MIDATA (2021). Retrieved from <https://www.MIDATA.coop/en/partners/>

¹²⁶ Corporate law of Switzerland is primarily contained within the Swiss Code of Obligations, from Article 552 to 1186. Cooperatives such as MIDATA are governed as per provisions under Article 828 to 926.

Significantly, members of the cooperative govern the use of data through a system of rights vested within Article 4 of MIDATA's Articles of Association.¹²⁷

Members of the cooperative are required to pay a one-time fee of CHF 40 to cover administration and operational costs incurred for managing the cooperative.¹²⁸ Private investments, including grant money, seem to constitute its primary source of funding.

Stakeholders

Individuals who hold an account on the MIDATA platform and members of the MIDATA cooperative are the primary data producers in this context. The nature of data stored and managed through the MIDATA platform is primarily personal data, including sensitive health information such as genomic data and medical records. They consent to share their data on a per-project basis with pharmaceutical companies, research institutions and other interested third parties that make up the category of data requestors.¹²⁹

Governance principles

Data sharing decisions undergo two levels of review and authorisation. First, every proposal containing a request for data is reviewed by MIDATA's Data Ethics Review Board.¹³⁰ The board may choose to admit a proposal, depending on the nature and purpose of research involved. Creating value for MIDATA's members and data account holders whilst contributing to society's knowledge on a particular health condition is a crucial consideration in the process of review. Second, the proposal that has been vetted by the Board is then sent to the general assembly of members for further authorisation. The general assembly follows a 'one member, one vote' model typical of cooperatives and a simple majority vote is necessary to gain approval for a proposed project.¹³¹

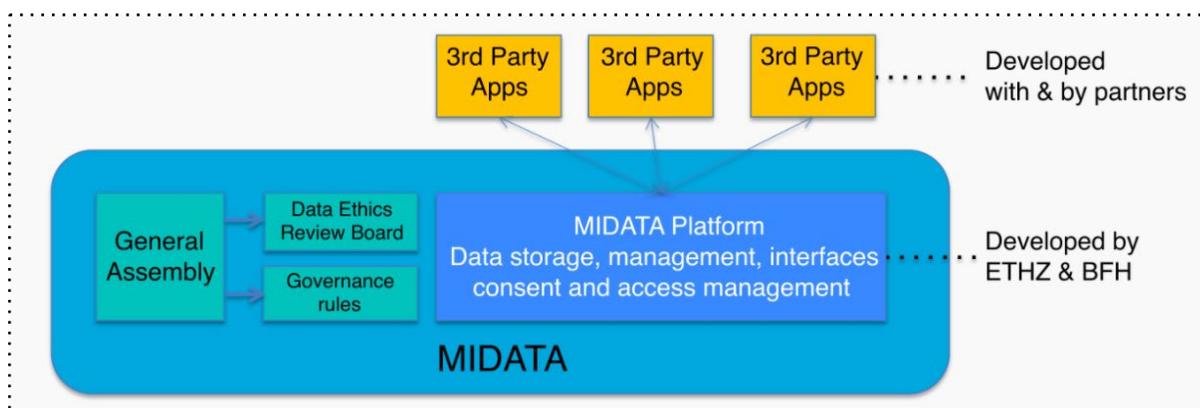


Figure 8: Governance mechanism of MIDATA (Source: MIDATA website)

Individual members and data account holders on the platform may consent to independently and exclusively share their personal data (or a specific subset therein) with other account holders, the cooperative itself or third parties requesting data.¹³² Consent collection is digitally-mediated and obtained through the MIDATA

127 The original MIDATA Article of Association, published in German, can be accessed here - https://www.MIDATA.coop/wp-content/uploads/2019/08/MIDATA_Stauten_20190626.pdf ; an unofficial English translation is also available on the website, viewable on https://www.MIDATA.coop/wp-content/uploads/2019/08/MIDATA_Stauten_20190626_EN.pdf

128 MIDATA (2021). Retrieved from <https://www.MIDATA.coop/en/faq/>

129 Stewardship Navigator (2021), Aapti Institute, <https://thedataeconomylab.com/> (pending publication)

130 Ibid.

131 Hafen, Ernst [Aapti Institute] (2020). "Data Economy Lab | Tracking stewardship: MIDATA - Unlocking value and control over our health data" [Video]. Youtube. <https://youtu.be/MfnDX-Sswr4>

132 Stewardship Navigator (2021), Aapti Institute, <https://thedataeconomylab.com/> (pending publication)

platform. Data producers (i.e. individuals) reserve the right to revoke consent for data use through the process of research and beyond.¹³³

Privacy controls

All data on the MIDATA platform is stored centrally on servers in Switzerland and follow multi-level encryption and 'a perfect forward secrecy protocol'.¹³⁴ Individual data may or may not be anonymised or pseudonymised prior to sharing, varying on the proposal under consideration and the nature of data required to undertake research. Third party data requestors are granted access to granular datasets of individuals who consent to sharing data for a specific project, after obtaining necessary authorisation for the project from the Data Ethics Review Board and the general assembly.¹³⁵

Analysis

MIDATA is founded on traditional cooperative principles that have been transposed onto the current data-driven world. It creates an environment for cooperative members to pool their data and use it in pursuit of their collective desires. Sophisticated standards for health data interoperability followed by MIDATA combined with a direct democracy approach to data sharing help achieve transparency and utmost technical safeguards for responsible bottom-up stewardship. Authorisation layers in the nature of MIDATA's Data Ethics Review Board help ensure compliance with community interests and that the members of the cooperative are involved at every step of the data value chain. Lastly, the not-for-profit nature of MIDATA avoids any conflict of interests that may arise when financial imperatives are posed against public good solutions.¹³⁶

3.5 Insights from case studies

The experiences of Driver's Seat, Open Humans and MIDATA chronicled in this section surface valuable reference points on the subject of data trusts and data trust-like initiatives. Although there exists significant differences in their structure - MIDATA and Driver's Seat are data cooperatives while Open Humans is a non-profit - the three use-cases nonetheless deliberately focalise community empowerment as the underlying purpose of their initiatives.

By examining real-world case studies, the research demonstrates the multiplicity of avenues and design choices that are available to builders of data trusts and data trust-like initiatives to actualise bottom-up mechanisms for stewardship. Further, it illustrates how initiatives managing the use of data can embed participation of data generators as a cornerstone of their governance principles. This marks a crucial departure from the current disempowering paradigm of data sharing that is opaque,¹³⁷ extractive¹³⁸ and marginalises the role of individuals and communities in data decisions.¹³⁹

These case studies highlight the virtues of bottom-up stewardship. Data sharing decisions within the use-cases considered go hand-in-hand with respect for agential rights of individuals and creation of social benefit through the use of data. Responsible data stewardship makes available data for social benefit in ways that are democratic and privacy-preserving, while balancing complex considerations of market incentives and public welfare.¹⁴⁰ Thus, upcoming data trusts and data trust-like initiatives should embody participatory

133 Ibid.

134 Ibid.

135 Ibid.

136 Kapoor, Aapti Institute (2021), "Rethinking data monetisation", <https://thedataeconomylab.com/2021/06/14/rethinking-data-monetisation/>

137 Engler, Brookings (2021), "Tech cannot be governed without access to its data", <https://www.brookings.edu/blog/techtank/2020/09/10/tech-cannot-be-governed-without-access-to-its-data/>

138 Sadowski, The Reboot (2021), "The Internet of Landlords Makes Renters of Us All", <https://thereboot.com/the-internet-of-landlords-makes-renters-of-us-all/>

139 Medina, The Conversation (2021), "NHS data gathering: government plans to collect and share health records are hugely concerning – here's why", <https://theconversation.com/nhs-data-gathering-government-plans-to-collect-and-share-health-records-are-hugely-concerning-heres-why-162699>

140 Tenisson, et al., Open Data Institute and Bennett Institute for Public Policy (2020), "The value of data: Policy implications", https://www.bennettinstitute.cam.ac.uk/media/uploads/files/Value_of_data_Policy_Implications_Report_26_Feb_ok4noWn.pdf

mechanisms for stewardship that can engineer effective outcomes for all stakeholders - communities, private entities and the public at large.

4. Key findings and takeaways

The research generated the following key findings and takeaways on the global state of data trusts:

1. While there is emerging consensus around what functions a data trust should deliver, there remain questions about the specific operational strategies which can deliver these functions in practice.¹⁴¹ However, the research encountered a plurality of bottom-up data stewardship initiatives that enable groups to engage in data sharing for social benefit and embody features that are nonetheless similar and attributed to data trusts.
2. **There is general optimism about the potential of data trusts among people working on data stewardship.** Both practitioner and expert respondents to the survey described a positive outlook on data trusts as an approach to data stewardship. Indeed, many were eager - and in some cases impatient - to see real-world examples to begin to test the considerable theory behind them.
3. **The interest in data trusts as a form of data stewardship seems to be driven from Europe and North America.** The response to the survey - with 37 of the 45 respondents based in Europe and North America - suggests a relative maturity in terms of imagining new forms of data stewardship. This may be due to the existence of data protection regulations that afford data rights, such as the right to access and portability, which are prerequisites to actualise bottom-up initiatives (such as the ones featured here as case studies). This means the maturity of the data rights landscape needs to be borne in mind while recommended data trusts in different jurisdictions.
4. **The purpose for bottom-up data stewardship can differ significantly.** The examples examined in this research are markedly different in their purpose, and subsequently their legal forms, governance processes and business model. Initiatives such as MIDATA and Open Humans are driven by altruistic motivations for data sharing. On the other hand, initiatives such as Driver's Seat, Swash and Digi.me seek to financially compensate those that have contributed data by charging interested parties for access.
5. **There are a number of real-world initiatives that demonstrate multiple routes to realising bottom-up data stewardship.** The survey findings and case studies exhibit a diversity of initiatives united in their efforts to empower individuals and communities to steward data. This highlights that there is no 'one-size-fits-all' framework for operationalising participatory forms of data stewardship.

¹⁴¹ Data Governance Working Group (2021), Global Partnership for Artificial Intelligence, "Understanding data trusts", <https://ceimia.org/wp-content/uploads/2021/07/2021-07-09-GPAI-summary-understanding-data-trusts-updated.docx.pdf>

5. Endnotes

5.1 About Aapti, ODI, and GPAI

Aapti Institute is a public research firm that works at the intersection of technology and society, building policy-relevant and actionable insights on the digital economy. It was founded in 2019 in Bangalore, India. Through its Data Economy Lab, a flagship effort to rebalance power in the digital economy, Aapti supports research, conversation and experimentation around the practice of data stewardship.

The **Open Data Institute** works to make data work for everyone by working with businesses and governments to build an open, trustworthy data ecosystem. It is independent, nonprofit and nonpartisan, founded in 2012 by Sir Tim Berners-Lee and Sir Nigel Shadbolt. From its headquarters in London and via its global network of startups, members and nodes, the ODI offers training, research and strategic advice for organisations looking to explore the possibilities of data.

The **Global Partnership on Artificial Intelligence (GPAI)** is a multi-stakeholder initiative which aims to bridge the gap between theory and practice on AI by supporting cutting-edge research and applied activities on AI-related priorities. Built around a shared commitment to the OECD Recommendation on Artificial Intelligence, GPAI brings together engaged minds and expertise from science, industry, civil society, governments, international organisations and academia to foster international cooperation.

5.2 Authors

This report was written by Astha Kapoor & Soujanya Sridharan from Aapti Institute and Jack Hardinges and Joe Massey from the Open Data Institute. The report was written in collaboration with the GPAI Data Working Group, whose insight and expertise helped to shape the direction, content and focus of this report.

5.3 Report drafting

This report was written in the autumn of 2021, with the research taking place over the summer. The survey was developed in July and distributed over the month of August which was followed by analysis and drafting of the report in September. The first draft of the report was reviewed by GPAI in late September.

5.4 Acknowledgements

We would like to thank GPAI for giving us the opportunity and funding to conduct this research and write this report, and for supporting the research with their knowledge and passion. We also thank the respondents who gave their time to answer the survey - their insights form the basis of this report.

6. Bibliography

6.1 Review of literature (academic papers, blogs, comments, news reports)

1. AI Council & Ada Lovelace Institute (2021, March 4). "Disambiguating data stewardship." *Ada Lovelace Institute*. Retrieved October 6, 2021, from <https://www.adalovelaceinstitute.org/blog/disambiguating-data-stewardship/>.
2. AI Council & Ada Lovelace Institute (2021, March 4). "Exploring legal mechanisms for data stewardship". *Ada Lovelace Institute*. Retrieved October 6, 2021, from <https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/>.
3. Andrejevic, M. (2009, September). "Privacy, Exploitation and the Digital Enclosure." *Amsterdam Law Forum*, 1 (4). Retrieved October 6, 2021, from https://www.researchgate.net/publication/228226821_Privacy_Exploitation_and_the_Digital_Enclosure.
4. Artyushina, A. (2020). "Is civic data governance the key to democratic smart cities? The role of the urban data trust in Sidewalk Toronto". *Telematics and Informatics, Volume 55*. Retrieved October 6, 2021, from <https://www.sciencedirect.com/science/article/pii/S0736585320301155>.
5. Artyushina, A. (2021, June 10). "The future of Data Trusts and the Global Race to dominate AI". *Bennett Institute for Public Policy*. Retrieved October 6, 2021, from <https://www.bennettinstitute.cam.ac.uk/blog/data-trusts1/>.
6. Bailey, R., & Goyal, T. (2019). "Fiduciary relationships as a means to protect privacy: Examining the use of the fiduciary concept in the draft Personal Data Protection Bill, 2018". *Data Governance Network Working Paper 04*. Retrieved October 6, 2021, from https://datagovernance.org/files/research/NIPFP_Rishab_Trishree_fiduciaries_-_Paper_4.pdf.
7. Balkin, J. M. (2020, November 18). "The fiduciary model of privacy". *SSRN*. Retrieved October 6, 2021, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3700087.
8. Barth, B. (2018, August 18). "The fight against Google's smart city". *The Washington Post*. Retrieved October 6, 2021, from <https://www.washingtonpost.com/news/theworldpost/wp/2018/08/08/sidewalk-labs/>.
9. Baruh, L., & Popescu, M. (2017). "Big data analytics and the limits of privacy self-management". *New Media & Society*, 19(4), 579–596. Retrieved October 6, 2021, from <https://doi.org/10.1177/1461444815614001>.
10. Beller, J. (2018). "The Message is Murder: Substrates of computational capital". *London: Pluto Press*. Retrieved October 6, 2021 from <https://doi.org/10.2307/j.ctt1x07z9t>.
11. Beuno, C. (2016, October 1). "The Attention Economy: Labour, Time and Power in Cognitive Capitalism". *London: Rowman and Littlefield International*.
12. Blankertz, A. (2020, February). "Designing Data Trusts: Why We Need to Test Consumer Data Trusts Now". *Stiftung Neue Verantwortung*. Retrieved October 6, 2021, from https://www.stiftung-nv.de/sites/default/files/designing_data_trusts_e.pdf.
13. Christopher, B. (2019, September 16). "Rentier capitalism: The UK case". *Bennett Institute for Public Policy*. Retrieved October 6, 2021, from <https://www.bennettinstitute.cam.ac.uk/blog/rentier-capitalism-uk-case/>.
14. Coyle, D. (2020, October 30). "Common governance of data: appropriate models for collective and individual rights". *Ada Lovelace Institute*. Retrieved October 6, 2021, from <https://www.adalovelaceinstitute.org/blog/common-governance-of-data/>.

15. Crouch, H. (2021, July 20). "GDPR September implementation date is scrapped". *Digital Health*. Retrieved October 6, 2021, from <https://www.digitalhealth.net/2021/07/gdpr-september-implementation-date-scrapped/>.
16. Data Governance Working Group (2021). "Understanding data trusts". *Global Partnership for Artificial Intelligence*. Retrieved October 6, 2021, from <https://ceimia.org/wp-content/uploads/2021/07/2021-07-09-GPAI-summary-understanding-data-trusts-updated.docx.pdf>.
17. Deming, D. (2021, February 19). "Balancing privacy with data sharing for the public good". *The New York Times*. Retrieved October 6, 2021, from <https://www.nytimes.com/2021/02/19/business/privacy-open-data-public.html>.
18. Dencik, L., & Kaun, A. (2020, June 23). "Datafication and the Welfare State". *University of California Press*. Retrieved October 6, 2021, from <https://online.ucpress.edu/gp/article-abstract/1/1/12912/110743/Datafication-and-the-Welfare-State?redirectedFrom=fulltext>.
19. Dickey, M. R. (2020, February 6). "Co-op helps Uber, Lyft drivers use data to maximize earnings". *TechCrunch*. Retrieved October 6, 2021, from <https://techcrunch.com/2020/02/06/co-op-helps-uber-lyft-drivers-use-data-to-maximize-earnings/>.
20. Dodds, L., Szász, D., Keller, J., Snaith, B., & Duarte, S. (2020, April). "Designing sustainable data institutions". *The Open Data Institute*. Retrieved October 6, 2021, from: <https://theodi.org/article/designing-sustainable-data-institutions-paper/>.
21. Element AI & Nesta (2019) "Data Trusts: A new tool for data governance". *Element AI*. Retrieved October 6, 2021, from https://hello.elementai.com/rs/024-OAQ-547/images/Data_Trusts_EN_201914.pdf
22. Engler, A. (2020, September 10). "Tech cannot be governed without access to its data". *Brookings*. Retrieved October 6, 2021, from <https://www.brookings.edu/blog/techtank/2020/09/10/tech-cannot-be-governed-without-access-to-its-data/>.
23. Forbes Technology Council (2019, September 3). "15 Social Challenges AI Could Help Solve". *Forbes*. Retrieved October 6, 2021, from <https://www.forbes.com/sites/forbestechcouncil/2019/09/03/15-social-challenges-ai-could-help-solve/?sh=76e9dd973533>.
24. Frist, B. (2021, January 20). "NIH Director Dr. Francis Collins: Connecting The Dots From The Human Genome Project To The COVID-19 Vaccine". *Forbes*. Retrieved October 6, 2021, from <https://www.forbes.com/sites/billfrist/2021/01/20/nih-director-dr-francis-collins-connecting-the-dots-from-the-human-genome-project-to-the-covid-19-vaccine/?sh=738447175438>.
25. Graham, M. (2019, October 2). "Lessons From a User-Trusted Data Trust". *DELL Technologies*. Retrieved October 6, 2021, from <https://www.delltechnologies.com/en-us/perspectives/lessons-from-a-user-trusted-data-trust/>.
26. Grueber, M., & Tripp, S. (2011, May). "Economic Impact of the Human Genome Project". *Battelle Memorial Institute*. Retrieved June 6, 2021, from <https://www.battelle.org/docs/default-source/misc/battelle-2011-misc-economic-impact-human-genome-project.pdf?sfvrsn=6>.
27. Gyeonggi-Do (2020, February 20). "Gyeonggi Province Becomes First Local Autonomy in World to Implement a Data Dividend; Governor Lee Jae-myung Says It "Heralds an Era of Data Sovereignty"". *Gyeonggi-Do*. Retrieved October 6, 2021, from <https://english.gg.go.kr/blog/daily-news/gyeonggi-province-becomes-the-first-municipality-in-the-world-to-implement-a-data-dividend-governor-lee-jae-myung-says-it-is-the-beginning-sign-of-the-era-of-data-sovereignty/>.
28. Hardinges, J. (2020, May 17). "Data trusts in 2020". *The Open Data Institute*. Retrieved October 6, 2021, from <https://theodi.org/article/data-trusts-in-2020/>.

29. Hardinges, J., & Keller, J. R. (2021, January 29). "What are data institutions and why are they important?" *The Open Data Institute*. Retrieved October 6, 2021, from <https://theodi.org/article/what-are-data-institutions-and-why-are-they-important/>.
30. Hardinges, J., Wells, P., Blanford, A., Tennison, J., & Scott, A. (2019, April). "Data trusts: lessons from three pilots". *The Open Data Institute*. Retrieved October 6, 2021, from <https://theodi.org/article/odi-data-trusts-report/>.
31. Harper, D. (2016). "Sharing Public Health Data saves lives". *International Journal of Infectious Diseases*, 53, 24–25. Retrieved October 6, 2021, from <https://doi.org/10.1016/j.ijid.2016.11.067>.
32. Hulin, A.-S. (2021, July 14). "How can civil law jurisdictions support data trusts? The Quebec Example". *The Data Trusts Initiative*. Retrieved October 6, 2021, from <https://datatrusts.uk/blogs/how-can-civil-law-jurisdictions-support-data-trusts-the-quebec-example>.
33. Joshi, D. (2020, August 11). "Non-Personal Data: Examining Data Trusts?" *Centre for Law & Policy Research*. Retrieved October 6, 2021, from <https://clpr.org.in/blog/non-personal-data-what-is-data-trusts/>.
34. Kapoor, A. (2021, February). "Collective bargaining on digital platforms and data stewardship". *Friedrich-Ebert-Stiftung*. Retrieved October 6, 2021, from <http://library.fes.de/pdf-files/bueros/singapur/17381.pdf>.
35. Kapoor, A. (2021, June 14). "Rethinking data monetisation". *The Data Economy Lab*. Retrieved October 6, 2021, from <https://thedataeconomylab.com/2021/06/14/rethinking-data-monetisation/>.
36. Keller, J., & Hardinges, J. (2021, June 25). "What are bottom-up data institutions and how do they empower people?" *The Open Data Institute*. Retrieved October 6, 2021, from <https://theodi.org/article/what-are-bottom-up-data-institutions-and-how-do-they-empower-people/>.
37. Kop, M. (2021, April 3). "The Right to Process Data for Machine Learning Purposes in the EU". *Jolt Digest*. Retrieved October 6, 2021, from <https://jolt.law.harvard.edu/digest/the-right-to-process-data-for-machine-learning-purposes-in-the-eu>.
38. Lau Jia Jun, J., Penner, J. E., & Wong, B. (2019, September 23). "The basics of private and public data trusts". *SSRN*. Retrieved October 6, 2021, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3458192#.
39. Lawrence, N. (2015, March 5). "Beware the rise of the digital oligarchy". *The Guardian*. Retrieved October 6, 2021, from <https://www.theguardian.com/media-network/2015/mar/05/digital-oligarchy-algorithms-personal-data>.
40. Lawrence, N. (2016, June 3). "Data Trusts could allay our privacy fears". *The Guardian*. Retrieved October 6, 2021, from <https://www.theguardian.com/media-network/2016/jun/03/data-trusts-privacy-fears-feudalism-democracy>.
41. Lawrence, N., & Delacroix, S. (2019, October 1). "Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance". *International Data Privacy Law*. Retrieved October 6, 2021, from <https://academic.oup.com/idpl/article/9/4/236/5579842>.
42. Manohar, S. (2019). "Trust law, fiduciaries, and data trusts". *The Data Economy Lab*. Retrieved October 6, 2021, from https://thedataeconomylab.com/wp-content/uploads/2020/10/DataTrustsPpr_SM.pdf.
43. Manohar, S. (2020, July 31). "Data Sharing for Public Good: Theoretical Bases and Policy Tools". *The Data Economy Lab*. Retrieved October 6, 2021, from <https://thedataeconomylab.com/2020/07/31/data-sharing-for-public-good-theoretical-bases-and-policy-tools/>.

44. Manohar, S., Ramesh, A., & Kapoor, A. (2020, June 24th). "Data Stewardship – A Taxonomy." *The Data Economy Lab*. Retrieved October 6, 2021, from <https://thedataeconomylab.com/2020/06/24/data-stewardship-a-taxonomy/>.
45. Mathews, L. (2017, September 7). "Equifax Data Breach Impacts 143 Million Americans". *Forbes*. Retrieved October 6, 2021, from <https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/#6f6ed8d3356f>.
46. Maxson Jones, K., Ankeny, R., & Cook-Deegan, R. (2013) "The Bermuda Principles". *Duke University Center for Public Genomics*. Retrieved October 6, 2021, from <https://dukespace.lib.duke.edu/dspace/handle/10161/7407>.
47. McDonald, S. (2019, March 5). "Reclaiming data trusts". *Centre for International Governance Innovation*. Retrieved October 6, 2021, from <https://www.cigionline.org/articles/reclaiming-data-trusts/>.
48. McDonald, S. (2019, October 28). "The Fiduciary Supply Chain". *Centre for International Governance Innovation*. Retrieved October 6, 2021, from <https://www.cigionline.org/articles/fiduciary-supply-chain/>.
49. McFarlane, B. (2020, August 16). "Data Trusts and defining property". *Oxford Law Faculty*. Retrieved October 6, 2021, from <https://www.law.ox.ac.uk/research-and-subject-groups/property-law/blog/2019/10/data-trusts-and-defining-property>.
50. Medina, I. (2021, June 18). "NHS Data Gathering: Government plans to collect and share health records are hugely concerning – here's why". *The Conversation*. Retrieved October 6, 2021, from <https://theconversation.com/nhs-data-gathering-government-plans-to-collect-and-share-health-records-are-hugely-concerning-heres-why-162699>.
51. MIT Technology Review Insights (2020, March 26). "The global AI agenda: Promise, reality, and a future of data sharing". *MIT Intelligence Review*. Retrieved October 6, 2021, from <https://www.technologyreview.com/2020/03/26/950287/the-global-ai-agenda-promise-reality-and-a-future-of-data-sharing/>.
52. Montgomery, J. (2021). "International perspectives on data institutions: lessons for data trusts". *The Data Trusts Initiative*. Retrieved October 6, 2021, from <https://datatrusts.uk/blogs/international-perspectives-on-data-institutions-lessons-for-data-trusts>.
53. Montgomery, J. (2021). "Understanding the Data Governance Act: in conversation with Sylvie Delacroix, Ben McFarlane and Paul Nemitz". *The Data Trusts Initiative*. Retrieved October 6, 2021, from <https://datatrusts.uk/blogs/understanding-the-data-governance-act-in-conversation-with-sylvie-delacroix-ben-mcfarlane-and-paul-nemitz>.
54. Morozov, E. (2017, October 19-20). "Digital intermediation of everything: at the intersection of politics, technology and finance." *Council of Europe Portal*. Retrieved October 6, 2021, from <https://rm.coe.int/digital-intermediation-of-everything-at-the-intersection-of-politics-t/168075baba>.
55. Newman, N. (n.d.). "How Big Data Enables Economic Harm to Consumers, Especially to Low-Income and Other Vulnerable Sectors of the Population". *Federal Trade Commission*. Retrieved October 6, 2021, from https://www.ftc.gov/system/files/documents/public_comments/2014/08/00015-92370.pdf.
56. Niklas, J. (n.d.). "Digital Rights are Human Rights". *Digital Freedom Fund*. Retrieved October 6, 2021, from <https://digitalfreedomfund.org/article-22-the-right-to-social-security/>.
57. Ostrom, E. (2009, December 8). "Beyond Markets and States: Polycentric Governance of Complex Economic Systems". *Nobel Prize Lecture*. Retrieved October 6, 2021, from https://www.nobelprize.org/uploads/2018/06/ostrom_lecture.pdf.

58. O'Connor, S. (2016, September 8). "When your boss is an algorithm". *Financial Times*. Retrieved October 6, 2021, from <https://www.ft.com/content/88fdc58e-754f-11e6-b60a-de4532d5ea35>.
59. Patel, R. (2021, September 7). "Participatory Data Stewardship". *Ada Lovelace Institute*. Retrieved October 6, 2021, from <https://www.adalovelaceinstitute.org/report/participatory-data-stewardship/>.
60. Patnaik, A. (2021, February 15). "Rethinking Personal Data Regulation in India". *The New Indian Express*. Retrieved October 6, 2021, from <https://www.newindianexpress.com/opinions/2021/feb/15/rethinking-personal-data-regulation-in-india-2264123.html>.
61. Pozen, D. E., & Khan, L. M. (2019, December 10). "A skeptical view of information fiduciaries". *Harvard Law Review*. Retrieved October 6, 2021, from <https://harvardlawreview.org/2019/12/a-skeptical-view-of-information-fiduciaries/>.
62. Ramesh, A., & Kapoor, A. (2020, July 31). "Principles for Revenue Models of Data Stewardship". *The Data Economy Lab*. Retrieved October 6, 2021, from <https://thedataeconomylab.com/2020/07/31/principles-for-revenue-models-of-data-stewardship/>.
63. Reddy T, P. (2021, July 16). "Counterpoint: Solving India's judicial backlog requires a nuanced conversation". *Scroll.in*. Retrieved October 6, 2021, from <https://scroll.in/article/1000329/counterpoint-solving-indias-judicial-backlog-requires-a-nuanced-conversation>.
64. Ruhaak, A. (2019, November 13). "Data trusts: Why, what and how?" *Medium*. Retrieved October 6, 2021, from <https://medium.com/@anoukruhaak/data-trusts-why-what-and-how-a8b53b53d34>.
65. Sadowski, J. (2021, March 15). "The internet of landlords makes renters of us all". *The Reboot*. Retrieved October 6, 2021, from <https://thereboot.com/the-internet-of-landlords-makes-renters-of-us-all/>.
66. Sadowski, J., Viljoen, S., & Whittaker, M. (2021). "Everyone should decide how their digital data are used — not just tech companies". *Nature*, 595(7866), 169–171. Retrieved October 6, 2021, from <https://doi.org/10.1038/d41586-021-01812-3>.
67. Scott, K. (2018, April). "Data for public benefit - understanding patient data". *Understanding Patient Data*. Retrieved October 6, 2021, from https://understandingpatientdata.org.uk/sites/default/files/2018-04/Data%20for%20public%20good_0.pdf.
68. Sridharan, S., Manohar, S., & Kapoor, A. (2021, September 29). "Health Data Stewardship: Learning from use-cases". *The Data Economy Lab*. Retrieved October 26, 2021, from <https://thedataeconomylab.com/2021/09/29/health-data-stewardship-learning-from-use-cases/>.
69. Stucke, M. E. (2018, March 17). "Here Are All the Reasons It's a Bad Idea to Let a Few Tech Companies Monopolize Our Data". *Harvard Business Review*. Retrieved October 6, 2021, from <https://hbr.org/2018/03/here-are-all-the-reasons-its-a-bad-idea-to-let-a-few-tech-companies-monopolize-our-data>.
70. Sundarajan, P. (2020, August 21). "Role of data stewards in enhancing accountability". *The Data Economy Lab*. Retrieved October 6, 2021, from <https://thedataeconomylab.com/2020/08/21/role-of-data-stewards-in-enhancing-accountability/>.
71. Sur (2021). "Online medical platforms are playing fast and loose, collecting patient data", *Medianama*. Retrieved October 6, 2021, from <https://www.medianama.com/2021/09/223-india-digital-health-medical-platforms-data-consent-records/>. [Paywalled]
72. Szász, D. (2020, October 26). "Tackling climate change challenges through data access – Microsoft and the ODI". *The Open Data Institute*. Retrieved October 6, 2021, from <https://theodi.org/article/tackling-climate-change-challenges-through-data-access-microsoft-and-the-odi/>.

73. Taylor, L. (2017, November 1). "What is Data Justice? the case for connecting Digital Rights and Freedoms globally ". *SAGE Journals*. Retrieved October 6, 2021, from <https://journals.sagepub.com/doi/10.1177/2053951717736335>.
74. Tennison, J., et. al., (2020). "Value of Data Report - Bennett Institute for Public Policy" . *Bennett Institute*. Retrieved October 6, 2021, from https://www.bennettinstitute.cam.ac.uk/media/uploads/files/Value_of_data_Policy_Implications_Report_26_Feb_ok4noWn.pdf.
75. Thatcher, J., O'Sullivan, D., & Mahmoudi, D. (2016, December 1). "Data colonialism through accumulation by dispossession: New metaphors for daily data". *Environment and Planning D-Society & Space*, 34(6), 990-1006. Retrieved October 6, 2021, from <https://escholarship.org/uc/item/5bf9164g>.
76. Tisne, M. (2020, July 14). "The Data Delusion: Protecting individual data isn't enough when the harm is collective". *Luminate*. Retrieved October 6, 2021, from https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/the_data_delusion_formatted-v3.pdf.
77. Transport Scotland (n.d.). Retrieved October 6, 2021 from <https://www.transport.gov.scot/transport-network/ports-and-harbours/port-governance/>.
78. Tusikov, N. (2019, August 6). "'Urban Data' & 'Civic Data Trusts' in the Smart City". *Centre for Free Expression*. Retrieved October 6, 2021, from <https://cfe.ryerson.ca/blog/2019/08/'urban-data'-'civic-data-trusts'-smart-city>.
79. Vallance, C. (2021, June 6). "GP data sharing: What is it and can I opt out?". *BBC*. Retrieved October 6, 2021, from <https://www.bbc.co.uk/news/technology-57555013>.
80. Various authors (2021, January). "The Digital New Deal: Visions of Justice in a Post-Covid World". *Just Net Coalition and IT for Change*. Retrieved October 6, 2021, from <https://itforchange.net/digital-new-deal/pdf/>.
81. Verhulst, S., Ramesh, A., Young, A., Rabley, P., & Keefe, C. (2021, June 4). "Establishing a data trust". *PLACE*. Retrieved October 6, 2021, from <https://www.thisisplace.org/blog-1/introducingplace/establishing-a-data-trust>.
82. Vial, G. (2020, December 8). "The data problem stalling AI". *MIT Sloan Management Review*. Retrieved October 6, 2021, from <https://sloanreview.mit.edu/article/the-data-problem-stalling-ai/>.
83. Viljoen, S. (2020, November 11). "A Relational Theory of Data Governance". *Yale Law Journal*. Retrieved October 6, 2021, from, <https://ssrn.com/abstract=3727562>. [Forthcoming]
84. Wilson, D. S. (2016, October 29). "The Tragedy of the Commons: How Elinor Ostrom Solved One of Life's Greatest Dilemma"s. *Economics*. Retrieved October 6, 2021, from <https://economics.com/tragedy-of-the-commons-elinor-ostrom/>.
85. Wylie, B., & McDonald, S. (2018, October 9). "What is a Data Trust?" *The Centre for International Governance Innovation*. Retrieved October 6, 2021, from <https://www.cigionline.org/articles/what-data-trust/>.
86. Zarkadakis, G. (2020, November 10). "'Data Trusts' Could Be the Key to Better AI". *Harvard Business Review*. Retrieved October 6, 2021, from <https://hbr.org/2020/11/data-trusts-could-be-the-key-to-better-ai>.
87. Zuboff, S. (2019, Jan 15). "The Age of Surveillance Capitalism: The Fight for Human Future at the New Frontier of Power". *New York: Public Affairs*.

6.2 Policy, regulation and strategy documents

Legislation/policy/ strategy documents	Jurisdiction	Link
Proposals to modernize Protection of Personal Information and Electronic Documents Act, 2020	Canada	https://news.ontario.ca/en/release/57985/ontario-launches-consultations-to-strengthen-privacy-protections-of-personal-data
Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 2020	European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767
Regulation (EU) 2016/679 of the European Parliament and of the Council - General Data Protection Regulation, 2016	European Union	https://eur-lex.europa.eu/eli/reg/2016/679/oj
Entering the new paradigm of artificial intelligence and series (strategy document), 2019	European Union	https://rm.coe.int/eurimages-entering-the-new-paradigm-051219/1680995331
Report by the Committee of Experts on Non-personal Data Governance Framework, 2020	India	https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf
Growing Artificial Intelligence Industry in the UK, 2017 (strategy document)	United Kingdom	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf
Investigation of Competition in Digital Markets: Department of Justice - Subcommittee on Antitrust, Commercial and Administrative Law, 2020	United States of America	https://judiciary.house.gov/uploaded_files/competition_in_digital_markets.pdf?utm_campaign=4493-519

6.3 Tools, guides and videos

Name	Author / publisher	Type	Link
Stewardship mapper	Aapti Institute	Tool	https://thedataeconomylab.com/mindmap/
Tracking stewardship	Aapti Institute	Videoù	https://thedataeconomylab.com/videos/
Stewardship Navigator (pending publication)	Aapti Institute	Database	https://thedataeconomylab.com/
A Human Rights-based Approach to Data	Office of the United Nations High Commissioner for Human Rights	Guide	https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf
Data protection and privacy legislations worldwide	United Nations Conference on Trade and Development	Tool	https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Output 2: Legal Review

Produced by:



In collaboration with:



Table of Contents

EXECUTIVE SUMMARY	49
INTRODUCTION.....	50
SECTION 1	51
1.1 The need for human centric approaches to data governance.....	51
1.2 Data trusts as a legal framework that can be transmuted for data.....	52
1.3 Challenges foreseen in implementation of data trusts.....	54
SECTION 2	57
2.1 Building a function-first framework for legal landscaping.....	57
2.2 Selecting jurisdictions - Gating criteria and challenges.....	62
2.3 Chronicling decisions/challenges :.....	63
SECTORAL INSIGHTS : Snapshots from across the globe	64
SECTION 3	67
3.1 : Background to Comparative analysis.....	67
SECTION 4.....	92

EXECUTIVE SUMMARY

This report forms one of two interlinked outputs supported by the Global Partnership for Artificial Intelligence (GPAI), centered around data trusts. This work takes a focussed look at the existing and necessary global legal landscape needed to enable data trusts. It aims to canvas global jurisdictions to assess their legislative data regimes, and provide a framework by which to evaluate the feasibility of data trusts in selected jurisdictions. In the conversation to enable data sharing and governance mechanisms that feed societal value, data trusts have been a focal point, particularly due to the degree of accountability that fiduciary duties in common law trusts can enable. To implement data trusts, however, numerous aspects require untangling - one of these is the legal applicability of trust law to the context of data, and related ecosystem-level needs, the focus of this report.

Beginning with a literature review that encompasses the bases and evolution of data trusts as a structure for human-centric data governance, this report posits the legal challenges foreseen in transmuting trusts for data. In order to carry out a global legal review, we developed a framework for necessary legal enablers as well as gating criteria for the jurisdictions considered in the analysis. This process and the challenges within it have been documented in this report. While the aim has been to encompass common law, civil code, and mixed legal systems - marrying them in a composite analysis framework is complex, as trust law and fiduciary duties feature most firmly and fundamentally in common law. Beyond the contours of fiduciary obligations, data rights, protection and sharing frameworks were also foregrounded as key enablers for data trusts - and each region has been evaluated upon these. Consequently, all eleven jurisdictions have been measured for their 'preparedness' to enable data trusts, and analysis for each has been detailed as well. While it is helpful to understand the data trust fertility across these regions, it has been a delicate balance to provide assessment while allowing for subjective interpretations of these legal landscapes, and the myriad (sociological, political and economic) nuances embedded in each region. Given this, the framework deploys a scale that moves from 'poorly defined' to 'robust'. It must be noted, however, that each of these data regimes are dynamic and evolving - implicitly, the analysis holds potential to be built upon and populated further. In many cases, our analysis has featured not only enacted legislation, but policy directives and other indicators of potential legal approaches to data governance.

This legal review has brought forth numerous insights - on parity across jurisdictions, the need for robust digital infrastructure, and the potential to embed different models of data stewardship, optimised for different contexts. Beyond the scope of legal analysis, challenges in implementing data trusts still remain. Building trust, establishing sustainable and beneficiary-oriented incentive structures, solving for notions of community data rights, and embedding meaningfully participatory governance in data trusts are a few of the questions that have followed from this research. It is hoped that the ecosystem of academics, policymakers, builders and civil society actors will build upon these questions and analyses, as data regimes and pathways to societal value crystallise in the coming years.

INTRODUCTION

The role of data in solving for some of the world's most pressing societal challenges - whether through healthcare, climate, mobility or scientific research - has become increasingly clear. Innovation is increasingly predicated in data-driven processes, and the success and conception of most artificial intelligence is defined too by data access and usability. In the shadow of this potential value, however, is a status quo reflecting stark inequities within the data economy - power is skewed toward large corporations and governments, while individuals and communities retain little visibility or agency into their data's journey, usage or governance.

As countries move to govern their data, regulation has shown a pronounced focus on the individual - on data protection, building robust consent frameworks and in some cases, instituting mature data rights like accessibility or portability. As this process unfolds across the globe, it is time to begin unpacking another important goal - empowering communities and enabling collectivisation to accrue the latent societal value of data. In recent years, scholars and practitioners have explored data trusts as a form of stewardship - one which envisions accountable and rights preserving pathways to both agency, and innovation-oriented value. While data stewardship has seen numerous instantiations, it has equally faced challenges of implementation. There is a need here, to examine how legislation may best enable community governance, and human-centric modes to manage our data.

In particular, data trusts are conceptualised upon existing common law pillars of trust law, and accountability instilled through fiduciary obligations. While this may present a compelling framework for delegated negotiation, collectivised leverage and responsible, streamlined data sharing - there are numerous lacunas in relying on trust law for data. It is in this context that we undertake an exercise in legal landscaping. The aim of this research, while nascent and largely unaccompanied by any sibling literature, is to provide a useful starting point and evaluation to understand the legal mechanisms that can enable data trust initiatives. Further, we analyse various global jurisdictions for their preparedness across these mechanisms - working through common and civil law systems, Global North and South countries, and countries at various stages in their data policy journeys. The breadth of this exercise has landed us at various permutations and combinations of preparedness, historical, legal and technical contexts across these regions. Thus, it is hoped that this analysis will serve as early literature to a growing body of work - how can data policy effectively enable trusted intermediaries and social benefit?

The following study adopts a function-first approach - using the actionable features assumed of a data trust to arrive at their corresponding legal pathways. At the outset, we establish the need for data stewardship, confine the term 'data trusts' to a single definition, and assess the foreseeable legal hiccups in implementation of the same. The weight of this work has been in its processes and comparative analysis - building a working framework for legal analysis by treading from roles of a trust, to functions, and arriving at necessary legal enablers. Beyond this, the selection of jurisdictions for analysis, and the application of a uniform framework to the vast global variety threw up a number of challenges - all of which we have attempted to chronicle in this report. While the analysis itself has yielded valuable insights, it is the authors' intention for this work to be built upon and multiplied - as the approaches and upshots of global data regimes steadily make themselves known.

SECTION 1

The report's introductory section traces data trust's theoretical and legal underpinnings, especially its reliance on common law trust frameworks. This has been carried out by a literature review, drawing on the works of various academics, practitioners, and organisations. The introduction is prefaced by discussions on the existing power imbalances in the data economy and the need to develop human-centric approaches to data governance.

Finally, building on these discussions, the final part of the section lays the foundations for the methodology and framework by outlining the various challenges that are foreseen in the implementation of data trusts. The key insights from the discussions in this section were as follows:

- Given the marked imbalances in the data economy, there is a growing realisation for the need to recognise data stewards that can preserve and advance the rights and interests of individuals.
- While there are different models of stewardship that can mediate these relationships, relying on trust law frameworks, data trusts represent a model of stewardship that places fiduciary responsibility at its heart.
- However, fitting data trusts in existing structures give rise to multiple challenges across legal systems that need to be explored.

1.1 The need for human centric approaches to data governance

In recent years, the rapid advancement of data-driven innovations and the computational tools that facilitate them has led to the development of a vast data economy.¹⁴² At the core of which lies the individual data subject; generating both personal data and non-personal community data.¹⁴³ However, the status quo of this economy reflects a fundamental power imbalance in the kinds of value being derived from such data drivenness. Value has been directed largely by market-first, profit oriented motives from private corporations, limiting not only the actualisation of data's societal value, but access to data itself. Consequently, individuals and communities are disadvantaged, unable to wield meaningful control over or partake in the governance, management and usage of their data. This asymmetry is both compounded by and symptomatic of the atomisation present in the data economy today - a fragmentation that creates no digital conception of communities. Data is relational, and shared lived experiences are often used in tandem to facilitate the weaponization of data. Further, it is now omnipresent in increasingly consequential decisions about users, workers, citizens, environmental and other resources, and the broader public. In many ways, data presents the new tool of exploitation.¹⁴⁴

There has been a steady global policy shift toward more privacy-oriented and rights preserving data governance - one that hopes to rebalance power toward the individual. With the EU's GDPR acting often as a median for other nations to build robust data protection, mature data rights like accessibility and portability are slowly finding voice. This has been simultaneous (though not necessarily equivalent) with the advent of community-oriented data intermediaries - data stewards.¹⁴⁵ A data steward can be defined as a trusted intermediary acting on behalf of data subjects or data generators, in their relationship with data requestors.

142McKinsey Global institute (2011), "Big Data : The next frontier for innovation, competition and productivity ", https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_exec_summary.pdf

143 In the context of this work, however, personal data trusts remain a primary focus.

144 Andrejevic (2009), Amsterdam Law Forum, "Privacy, Exploitation and the Digital Enclosure", https://www.researchgate.net/publication/228226821_Privacy_Exploitation_and_the_Digital_Enclosure

145 Manohar, Kapoor and Ramesh (2020), Aapti Institute, "Data Stewardship: A Taxonomy", <https://thedataeconomylab.com/2020/06/24/data-stewardship-a-taxonomy/>

As a body that acts in the interest of data subjects, stewards work to enable greater agency, transparency and protection for subjects, negotiate with data requesters, and seek avenues for societal benefit from data.

Thus, the role of a steward is dual: both rights preserving and value generative. Stepping beyond the paradigm of individual protection, stewardship strives to empower and circularise value chains¹⁴⁶ - not only for those who most crucially drive the data economy, but to use data as a leveller for pre-digital vulnerabilities in society. However, data is difficult to govern - its value is defined most critically by how it is used, this value is often dynamic over time, and different data types necessitate different rights, needs and management. Given these challenges, data stewardship embodies a diverse set of structures, most of which are problem-led, and seek to responsibly solve for sectoral or purpose driven goals. Many of these are currently being implemented in practice, and they are being robustly analysed as they evolve.¹⁴⁷ Section 1.2 introduces the concept of trusts as a potential legal framework for data.

1.2 Data trusts as a legal framework that can be transmuted for data

Some models for data stewardship draw from existing legal frameworks to implement various modes of community governance over different data types. For example, an increasingly prevalent stewardship structure, data cooperatives map to the traditional cooperative model. Members typically partake in decision making in a democratic one-member-one-vote structure, pool their resources (in this case data) and work to further a common societal or other goal. The Driver's Seat¹⁴⁸ cooperative provides platform workers on ride sharing platforms with useful analytics on their data, enabling greater transparency and agency over their daily wages - which are typically informed by this data but not shared with drivers. Once aggregated, these insights are also sold to local governance and transport agencies, the revenue from which is divided amongst the cooperative members.

Data trusts present another model that relies on an existing legal framework - based most foundationally in the concept of fiduciary responsibility. This will be elucidated further in this study. While common law trusts most broadly denote a transference or delegation of rights, ownership or some kind of property to a fiduciary (trustee), the structure for *data* trusts has differed across many thinkers and this discourse remains dynamic. For the purpose of this research, data trusts are defined as 'A form of data stewardship that supports data producers to pool their data (or data rights) to collectively negotiate terms of use with potential data users, through the oversight by independent trustees, with fiduciary duties, and within a framework of technical, legal and policy interventions that facilitate data use and provide strong safeguards against misuse.'¹⁴⁹

There are other approaches to data stewardship, such as Data Commons, which are not embedded in law but only in practice. However, the focus on legal perspectives, and particularly on data trusts, is informed by the high levels of accountability that law can provide. In this context, we explore the conception of data trusts and how it has evolved - beginning at the notion of information fiduciaries, and the possibility of heightened accountability for data controllers.

A fiducial view of data governance

Scholars like Balkin¹⁵⁰ and Tuch¹⁵¹ identify an increasing dependency and vulnerability toward big technologies as functionally similar to traditional fiduciary relationships that individuals have with doctors and lawyers. Fiduciary relationships typically involve some exercise of discretionary power over the interests of the recipient/beneficiary. This power is authorised through consent, unilateral undertaking or legal decree.¹⁵² To address this imbalance between individuals and technology corporations, they rely on conventional fiduciary principles to propose recognising big technological corporations that depend on data-driven

146 Mc Donald, S (2019), Centre for International Governance Innovation, "The Fiduciary Supply Chain", <https://www.cigionline.org/articles/fiduciary-supply-chain/>

147 The Data Economy Lab, Aapti Institute, "Tracking Stewardship", <https://thedataeconomylab.com/tracking-stewardship/>

148 See <https://driversseat.co/>

149 Data Governance Working Group (2021), Global Partnership for Artificial Intelligence, "Understanding data trusts", <https://ceimia.org/wp-content/uploads/2021/07/2021-07-09-GPAI-summary-understanding-data-trusts-updated.docx.pdf>

150 Balkin, Jack M (2016), UC Davis Law Review, "Information Fiduciaries and the First Amendment", Available at SSRN: <https://ssrn.com/abstract=2675270>

151 Tuch, Andrew F (2020), Washington University Law Review 1897 (2021), "A General Defense of Information Fiduciaries", Available at SSRN: <https://ssrn.com/abstract=3696946>

152 Miller, P (2014), Oxford University Press, "The Fiduciary Relationship"

algorithmic processing as 'information fiduciaries'.¹⁵³ Depending on the nature of their relationship with users, these information fiduciaries, Balkin argues, ought to be bound by fiduciary duties to impose a higher standard of care - one that ensures the prevention of harm towards consumers.¹⁵⁴

Balkin's classification of information fiduciaries gathered support from academics, lawmakers, and technology companies. However, attempts to embed these ideas of trust and fiduciary duty in regulating data rights¹⁵⁵, have failed to define obligations that address these imbalances. For instance, the Indian Personal Data Protection Bill's conception of a data fiduciary - which is the GDPR equivalent of a data controller - except when dealing with children's data, does not require data fiduciaries to make decisions that prioritize the data subjects' interests.

However, scholars like Khan, Pozen, and Grimmelmann - while in agreement with the underlying recognition of the asymmetry of information and control - are critical of this approach. Khan and Pozen contend that imposing a higher standard of care on corporations - owing to their divided loyalties to shareholders and consumers - is antithetical to fiduciary law.¹⁵⁶ Grimmelmann further adds to this shortcoming by noting that defining the contours of loyalty for information fiduciaries has its limitations; it either risks being too rigid or too broad.¹⁵⁷

Addressing the concerns posed by Khan et al., Delacroix and Lawrence, rely on the common law conception of trusts - envisaging data trusts as a form of bottom-up data governance wherein data subjects pool their data rights for a common purpose.¹⁵⁸ Part of the reason why legal trusts have captured current discourse around data stewardship, when thinking about accountability, is because of the fiduciary obligations that trustees have towards their beneficiaries. While the exact nature of fiduciary duties vary across jurisdictions, at the heart of it, fiduciaries must act with utmost loyalty towards the beneficiaries. The common law notion of trust involves the administration of privately owned assets by independent trustees who act on behalf of the beneficiaries identified by the asset owner.¹⁵⁹

Data trusts propose the appointment of independent trustees - which owe a fiduciary duty to these subjects - to make impartial decisions on the collectivized pool of rights. Fiduciary duty entails a high level of accountability, particularly because there is a disparity in power between trustees and beneficiaries. In most cases, this also means that courts are enabled to intervene in the functioning and structure of a trust at a normative level, allowing greater oversight to the benefit of subjects. The trustee, therefore, cannot use the asset for their own personal gain. These structures seek to enhance individual control over personal information.¹⁶⁰

While the conception of data trusts draws from principles of equity and trusts, the use of data trusts so far has been theoretical, and the legal and regulatory frameworks on which data trusts may stand on are yet to be defined. Any policy intervention, therefore, requires a granular identification of the mechanisms that can instantiate data trusts. At the outset of such an exercise, it is important to first identify the existing gaps and challenges in implementing the features of trust law within the context of data.

153 Balkin 2016 (n 4)

154 *ibid.*

155 US Senator for Hawaii Brian Schatz (2018), "Schatz Leads Group of 15 Senators In Introducing New Bill To Help Protect People's Personal Data Online" Available at <https://www.schatz.senate.gov/news/press-releases/schatz-leads-group-of-15-senators-in-introducing-new-bill-to-help-protect-peoples-personal-data-online>

156 Khan L., and Pozen D (2019), Harvard Law Review, "A Skeptical View of Information Fiduciaries"

157 Grimmelmann J (2019), Law and Political Economy Blog, "When All You Have is a Fiduciary" Available at <https://lpeproject.org/blog/when-all-you-have-is-a-fiduciary/>

158 Delacroix S., and Lawrence N (2019), International Data Privacy Law, "Disturbing the "One Size fits All" approach to Data Governance: Bottom-up Data Trusts."

159 *Knight v Knight* (1840) 49 ER 58

160 Mc Donald, S (2019), Centre for International Governance Innovation, "Reclaiming Data Trusts" Available at Reclaiming Data Trusts - Centre for International Governance Innovation (cigionline.org)

1.3 Challenges foreseen in implementation of data trusts

In order to assess the possible implementation of data trusts, we have examined and distilled the key challenges that are likely to arise, which this section details. From a legal perspective, these range from conceptions of fiduciary duty and means for accountability to the subject matter and assignment of data rights to trustees. Beyond these, there remain other challenges to implementation around sustainability and incentive structures. While these are pertinent questions, they do not feature in this review, which is limited to foundational legal tools that may facilitate data trusts.

a) Fiduciary duties

Central to the idea of bottom-up data trusts is the management of the rights of the data holders in the interests of data providers. Trustees are, therefore, bound by a fiduciary responsibility that is underpinned by undivided loyalty towards their beneficiaries.¹⁶¹ Undivided loyalty requires the fiduciary to place the beneficiary's interests over their own and not have any interests that come in conflict with this.¹⁶² It is important to note that the identification of fiduciary relationships is context specific and jurisdiction specific.¹⁶³ The nature of fiduciary responsibility may also vary according to the relationship; the fiduciary duty owed by a lawyer to a client may vary from the one owed by a trustee to its beneficiary. And, across common law jurisdictions, fiduciary duty has a higher expectation of good faith than the common law conception of 'reasonable care'.¹⁶⁴

Given the historical distinction in common law between courts of law and courts of equity, fiduciary principles developed distinctly as a product of equity. Civil law systems do not make this distinction. Any exploration of the legal frameworks for data trust, needs to be wary of the limitations in relying solely on the common law conception of trusts. Notwithstanding a few civil jurisdictions that have either ratified the Hague Trust Convention¹⁶⁵ or codified trusts within their legal systems, most civil law jurisdictions do not recognise legal trusts. Envisaging data trusts in these settings will require careful consideration of the fiduciary responsibilities that data trusts seek to represent and identify functional equivalents of fiduciary-like principles of trustee-beneficiary relationships across these different legal systems.

b) Accountability Mechanisms

The recognition of a fiduciary relationship under trust law also ensures accountability mechanisms within the design of these trusts. A fiduciary relationship is essentially "one in which one party (the fiduciary) exercises discretionary power over the significant practical interests of another (the beneficiary)".¹⁶⁶ Within legal trusts, beneficiaries hold trustees to account by bringing claims against trustees if they feel treated unfairly or dishonestly.¹⁶⁷

Similarly, accountability mechanisms can also be located in corporate structures through company's annual general meetings and provisions that allow the removal of directors. However, in most instances, directors owe fiduciary duties towards the company and not the shareholders.

Furthermore, in legal trusts, the court's equitable jurisdiction gives it broader powers to redress harms arising in fiduciary relationships. However, it needs to be explored how such functional frameworks can be transposed to or identified in jurisdictions that do not have such legal structures.

c) Identifying the subject matter of the trust

Even within the current discourse on building data trusts in common law systems, there are differing viewpoints on the reliance of legal trust structures to instantiate data trusts. The ODI's report on legal and governance considerations contends that subject-matter requirements for legal trusts impede the conception of data trusts within the existing legal framework. The report asserts that data is not capable of being

161 Delacroix and Lawrence (n 12)

162 Bristol & West Building Society v Mothew per Millet LJ

163 Miller, Paul B (2018), the Oxford Handbook of Fiduciary Law, "The Identification of Fiduciary Relationships", Available at SSRN: <https://ssrn.com/abstract=3119136>

164 Clarry, D(2014), International and Comparative Law Quarterly, Fiduciary Ownership And Trusts In A Comparative Perspective." doi:10.1017/S0020589314000463

165 Hague Trust Convention is a multilateral treaty that harmonizes a trust's definition and clarifies the choice of law and applicable rules for governing trusts. Currently, 14 countries have ratified the convention.

166 Miller, P (2014), Oxford University Press, "The Fiduciary Relationship"

167 See Keech v Sandford where the court found the trustee liable for acting in conflict of interest.

constituted as property “in the legal trust sense” and, therefore, ‘cannot form the basis of a legal trust’.¹⁶⁸ However, Delacroix and Lawrence, and Lau, Penner, and Wong, in their responses point out that even if this assertion of data not being property is made owing to its intangible nature, it does not hold ground as common law jurisdictions recognise intangible trade assets and bank accounts (the right to payment against a bank) as a subject matter of trusts.¹⁶⁹

McFarlane makes a larger point on how it is inconsequential as to whether data is property or not.¹⁷⁰ ‘Property’ in the legal sense reflects different ideas in different contexts, and when imagining legal frameworks for data trusts, rather than examining whether a thing is data or not it is important to unbundle the scope rights over different data. McFarlane illustrates this through a scenario where B is owed a certain amount of money from A arising out of a contract between the two. In this context, the contractual right in itself is not a property. However, the rights to receive the money owed are perfectly capable of being held in trust. Unlike rights that define individuals by virtue of their identity as a right holder - for instance a professional license or a qualification - data rights are not intrinsically linked to a particular individual in the same manner.¹⁷¹

Therefore, under English law, the question of what can be held in data trusts depends on the type of data and the range of positive rights available over it. This also raises questions on how these pooled rights interact with each other, and the extent to which they can be disaggregated. It is important to note that even in jurisdictions that recognise trusts, the conception of what can be held as the subject-matter of trusts varies.

d) Delineating the duties and interests of trustees and beneficiaries of the trust

There are also challenges to how one defines beneficiaries (and their interests) and trustees (and their obligations). The scope of definitions of who or what group constitutes a beneficiary has implications on fiduciary actions.¹⁷² The ODI report asserts that sharing data for public benefit could be a breach of fiduciary duty as trusts in English law requires “the trustees to allow data to be shared only for the benefit of a defined group of beneficiaries”. The only exception, the report notes, are charitable trusts, which can operate for public benefit. However, the report falls short of exploring them as it would only be “suitable for a minority of data trusts”.¹⁷³ However, it is worth noting that charitable trusts in commonwealth jurisdictions such as England, India and Australia are exempt from the beneficiary principle, i.e., they do not need to have identified beneficiaries, and can operate for the general benefit of the public in furtherance of an (abstract) purpose.

The ODI Report also observes that trustees’ obligations not to use the property of the legal trust in a manner that benefits themselves can create hurdles for beneficiaries (data providers) to be trustees. This is not entirely accurate as trustees – under common law - can also be beneficiaries of a trust if they are not the sole beneficiary.¹⁷⁴ Trustees, in fact, can be remunerated for their services insofar as they are not unauthorised or secret profits obtained because of their position.

168 Reed C (2019), BPE solicitors and Pinsent Masons, “Data trusts: Legal and Governance Considerations” Available at <https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf>

169 Lau Jia Jun, J., Penner, J., and Wong, B (2019), NUS Law Working Paper, “The Basics of Private and Public Data Trusts” Available at SSRN: <https://ssrn.com/abstract=3458192> or <http://dx.doi.org/10.2139/ssrn.3458192>

170 McFarlane, B (2019), University of Oxford, “Data Trusts and Defining Property” Available at <https://www.law.ox.ac.uk/research-and-subject-groups/property-law/blog/2019/10/data-trusts-and-defining-property>

171 Delacroix and Lawrence (n 12)

172 Mc Donald, S (2019), Centre for International Governance Innovation, “Reclaiming Data Trusts” Available at Reclaiming Data Trusts - Centre for International Governance Innovation (cigionline.org)

173 Reed C (2019), BPE solicitors and Pinsent Masons, “Data trusts: Legal and Governance Considerations” Available at <https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf>

174 Lau, Penner, and Wong (n 20)

e) Assigning data rights to third parties

In most jurisdictions, individual rights relating to data are sourced from data protection laws and the recognition of fundamental rights within the constitution.¹⁷⁵ Data protection laws such as the GDPR, the LGPD, and the CCPA recognise certain positive rights around access, use, erasure, and data portability. Whether current data protection laws allow the assignment of these rights to a third-party (the data trust) is an area which remains to be explored.

Concurrently, personal data protection laws will also have a bearing on data trusts that fall within a specific jurisdiction. The plurality of bottom-up data trusts and the flexibility in the governance structures of these data trusts mean that the obligation and compliance requirements of a data trust will be dictated by the objects of the specific data trust and the definitions used under the relevant personal data protection laws¹⁷⁶. The GDPR, LGPD, and PDPB for instance, make a distinction between a data controller¹⁷⁷ who determines the purpose and means of processing; and a data processor who merely “processes personal data on behalf of the controller”. Data controllers have broader and more onerous responsibilities than data processors. The Canadian PIPEDA, on the other hand, does not make this distinction.

The interplay of various rights within bottom-up data trusts could also pose new questions on the current framing of data rights. Collectivised management of data rights under the trust framework would require balancing conflicting rights and even the recognition of new data rights altogether. The idea of community rights to data advanced by India’s Ministry of Electronics and Information Technology’s (MeitY) report on Non-Personal Data (NPD) is a case in point.¹⁷⁸ The NPD framework proposes collective rights to privacy over community non-personal data - in contrast to the framing of rights over personal data where the individual is the focal point of data protection.

At the most basic level, for data trusts that make decisions on the purposes and means of processing data, it remains to be seen how they will be affected by the notice and consent requirements specified under various data protection laws. This is particularly relevant for data trustees and third parties when processing personal data of individuals and communities. Similarly, the principle of purpose limitation may pose challenges for trustees to share data meaningfully.

Having identified the challenges, it is evident that the instantiation of data trusts merit analysis that addresses questions on the representation of data rights by intermediaries bound by fiduciary responsibility. Consequently, it is essential to explore the legal landscape of data rights and legislative frameworks across different jurisdictions to identify opportunities and gaps in the development of data trusts. Section 2 sets forth the methodology and approach, detailing the considerations that went into framing our analysis.

Can data rights form the subject matter of trusts across jurisdictions?

Identifying what can constitute the subject matter of a trust is essential to the creation of data trusts. However, the evolution and reliance on the trust framework within jurisdictions that have adopted the common law system has not been uniform. Many of these countries have codified provisions in ways that may have departed in some ways from the core principles of English law trusts. For instance, unlike England, India and South Africa do not recognise the concept of dual ownership for trusts. Similarly, while courts in England have recognised the ability for trusts to hold non-assignable contractual rights in trusts, it is not certain if this would apply to other jurisdictions that have legal trusts. For instance, section 8 of the Indian Trusts Act, defines subject matter of trusts as “property transferable to the beneficiary”. Whether trusts can hold data (or the rights over it) is a question that needs to be examined in greater detail in each of these jurisdictions.

175 For eg: South Africa and India recognise the right to privacy within their constitutions.

176 Subject to the data trusts jurisdiction of operation and the applicability of the relevant data protection legislation

177 The Indian PDP terms them as data fiduciaries with broadly similarly definitions

178 The Ministry of Electronics & Information Technology (2020), “Report by the Committee of Experts on Non-Personal Data Governance Framework” available at https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf

SECTION 2

Having reviewed the challenges in representing data trusts in the previous section, the following section presents the methodology and the resultant framework for the comparative analysis. The methodology develops a function-first approach, outlining the key roles of data trust as an intermediary in the data economy. Building on this, the framework identifies three legislative enablers necessary for creating data trusts that can fulfil these functions. The three enablers identified are as follows:

1. Data protection and rights
 2. Data sharing
 3. Fiduciary obligations
1. Geographical distribution
 2. Representation of the different legal systems; and
 3. Presence of data protection and sharing frameworks

However, given the complexity in comparing these enablers across such diverse legal systems, there were numerous challenges which the later parts of the section chronicle.

2.1 Building a function-first framework for legal landscaping

Methodology

Within the ambit of data stewardship models - such as cooperatives, unions, repositories, exchanges or personal data stores - data trusts present an explicitly legal challenge. While trust law presents potential as an existing legal tool for stewardship, there is a wider legislative environment required for trusts to manage data. As discussed above, aspects like fiduciary responsibility or the subject matter of a trust require untangling in order to make data trusts feasible. Consequently, differences in various legal systems, their foundations - whether common law, civil code, or mixed - and their historical contexts complicate such an analysis.

Further, theoretical definitions around data trusts and the roles embedded within them have been varied since their inception and continue to evolve. In order to take the concept of data trusts from abstract delineation-via-exclusion, it is necessary to arrive at the actionable features that follow from theoretical definitions of role or responsibility. Given these challenges, this research has adopted a function-first approach to legal analysis.

Role

Coalescing various definitions of the role or persona of data trusts informed the first leg of building an analysis framework. This has been based also on the consensus statement formulated by the Global Partnership on Artificial Intelligence, the works of Lawrence and Delacroix, the Ada Lovelace Institute and more as featured in the aforementioned literature review. The primary role of a data trust is to act as a trusted intermediary in the move towards a more equitable and agential data economy, particularly for data subjects and generators. Along with rebalancing power asymmetries, data trusts and stewards more broadly are envisioned to enable data-driven innovation for social benefit, and to preemptively protect subjects from potential vulnerabilities that arise from data management. These core ideals can be distilled into the following roles:

1. Protect

Data trusts must work both to preemptively protect beneficiaries from potential harms arising from the use or misuse of their data, as well as retroactively ensuring avenues for adequate recourse in the event of harm.

2. Empower

Protection alone does not necessitate agency. A key duty of a data trust, and of other data stewards, must be to empower beneficiaries through decision making, cognisance of data rights, and other means of participation in their data's management.¹⁷⁹

3. Generate value

As part of rebalancing power and value within data economies, data trusts must be primed to further broader social and public benefit from data sharing - primarily by promoting data driven innovation and facilitating trusted pathways and environments for the same.

4. Negotiate

The framework of a trust creates a dynamic where trustees are enabled to negotiate on behalf of beneficiaries. This also necessitates a level of skill and expertise in trustees such that they may compensate for asymmetries that hinge on the epistemic disadvantages often faced by data subjects.

5. Maintain accountability

In order for trustees to effectively prioritise beneficiaries interests, it is necessary to codify a high degree of accountability toward beneficiaries. This is enabled in part by fiduciary obligations, which entail duties of skill, care and loyalty toward beneficiaries, and also in allowing judicial intervention upon the failure of such obligations.

¹⁷⁹ These means differ across different models of stewardship and their governance/participation structures

Role → Function

In order to evaluate the feasibility of data trusts from a legal lens, it is important to focalise actionable features that correlate to the key roles of a trust. This analysis aims at taking structural analyses of data trusts to a functional level, and so entailed a delineation of tasks. It is important to note here that despite identifying various purposes for data trusts (and consequently, data types and beneficiaries), the functions of the data trust remain unchanged.

1. Provide clear and usable redressal mechanisms to beneficiaries in the event of misuse or harm.
2. Establish safeguards and oversight mechanisms to preemptively prevent misuse or harm.
3. Provide a platform for collectives to establish trust terms, conditions and constitution.
4. Proactively identify and define the subject matter of the trust and its use purpose.
5. Enable data sharing and work to make data available for social good through innovation.
6. Negotiate the use of trust assets with third parties, and facilitate safe and controlled access or use.
7. Appoint expert trustees (professional managers) as stewards, pertaining to the purpose scope and data types being managed.
8. Instil transparency mechanisms for accountability and loyalty from trustees toward beneficiaries.

In Figure 2.1.1, the correlations across roles and functions are depicted. The primary functions associated with data trusts are associated with a necessary level of expertise, trust and accountability. Certain functions act to support these features, such as platform creation and the identification of value pathways from data. However, it is only through the confluence of all eight that a data trust may be considered primed to fulfil its roles. Thus, while the enlisted functions and roles are necessary conditions for a data trust, there may be other factors that make up the sufficient conditions. For example, data trusts must be structured with incentive models that allow for sustained accountability, and financial models that allow for sustained revenue or sustenance of the trust. These aspects, discussed further in Section 4, are not necessarily facilitated function-first, or through legislative intervention and thus do not feature in our evaluation.

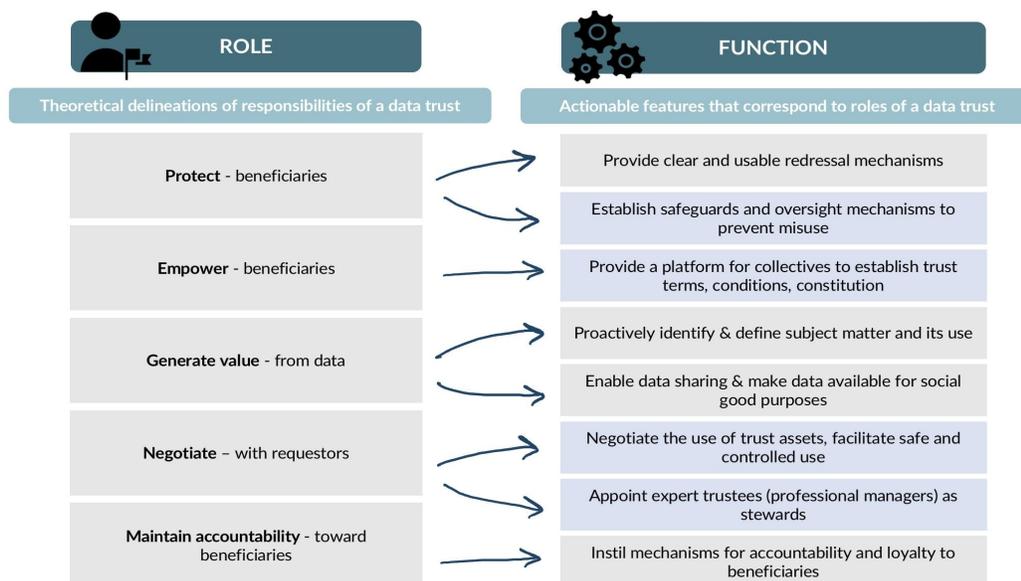


Figure 2.1.1 depicts the roles, functions of a data trust, as well as the embedded correlations between them

Function → Enabler

Having identified the core functions necessary for a data trust, there are three legislative arenas that can come together to enable such functions. Figure XX shows the logical flow from function to these three foundational enablers, which have each been elucidated below. Since most countries are still evolving their data regimes and governance strategies, some of these enablers remain unclear within certain jurisdictions - yet, they are an integral part of the preparation toward data trusts and thus necessary to this evaluation.

- Data rights and protection

In order to facilitate *any kind* of principal protection, intermediaries must be armoured with clear and robust digital rights and data protection that will allow them to actionise features around redressal and preemptive protection. It is also important to acknowledge that the regulation of data and the rights afforded to individuals may adopt sector-specific approaches. For instance, the USA regulates data processing through specific laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the Children's Online Privacy Protection Act (COPPA). While the HIPAA recognises access and portability rights over health data, the COPPA stipulates the processing limitations and consent requirements for children's data. In this analysis, data protection features as perhaps the most weighted enabler for data trusts. However, beyond individual or collective protection, mature data rights such as portability, findability and accessibility are also foundational to such structures. In order for data protection to translate to the intermediary, data rights must hold definitions around delegation, for trustees to be able to manage data on behalf of beneficiaries. As discussed above, while many hold that the subject matter of a trust may be the management of rights - it is unclear in many jurisdictions whether data rights (or their execution) are transferable at all, and to what extent. Individual protection must be coupled with individual autonomy over data and, for streamlined intermediaries - clarity on the delegation or exercise of such autonomy.

- Data sharing

Beyond data protection and data rights, data trusts are situated within a larger ecosystem of data - one that must be streamlined for data sharing if it is to generate societal value. By many accounts, the eventual vision of this ecosystem also includes a plurality of data trusts (for various purposes, types and subjects). Further, the function of enabling innovation and making data available also requires this broader network of varied data entities. Based on this, we have considered in our analysis the availability and lucidity of legal frameworks for data sharing. This ranges from regulation around data standards, formats, sectoral interplay, purpose limitations and sharing agreements - infrastructure-oriented policy that may seek to build ecosystem-wide technical capacity. Moves toward nationwide interoperability, data exchange networks, etc are technical elements that can work to build trusted networks for data trusts to rely on. In order to efficiently define data types and purposes within a trust, legislation and broader policy efforts alike must also be lucid on the limitations and definitions of aspects like 'public good,' or 'innovation purpose'.

- Fiduciary obligations

Common law trusts, which may be considered the parent legal framework for data trusts, have been most effectively buttressed by conceptions of fiduciary responsibility. Fiduciary duties under common law, as discussed in Section 1, allow for levels of accountability and loyalty that many would argue are difficult to institute contractually. Further, fiduciary duty attempts to mitigate and give legislative importance to the power asymmetry associated with a delegation of rights, ownership or more - particularly given the expertise that a trustee retains in comparison to the typical beneficiary. Thus, this has been the third key enabler as we evaluate global jurisdictions. However, there is a marked need to recognise that not all fiduciary duty (across jurisdictions) can be read identically, and may be very different in implementation. And in the absence of fiduciary duty under law (which is the case for many regions globally) it is important to consider other pathways for similar degrees of accountability, loyalty and potential judicial intervention. These considerations find mention in our comparative analysis (Section 3) as well as our application of the framework (Section chronicling challenges)

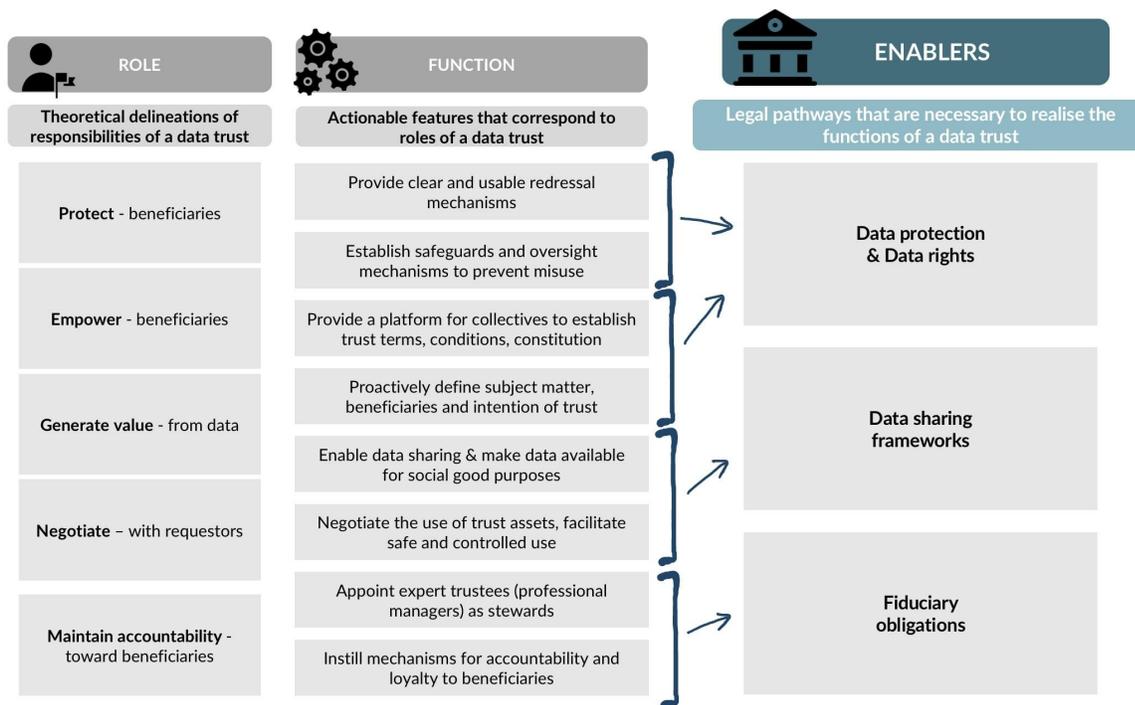


Figure 2.1.2 depicts the move from functions of a data trust, to the 3 key legal enablers that they require

Enablers → Metrics & Indicators

Our methodology builds on the three enablers to identify metrics and indicators required to activate the role and functions of the data trusts. For instance, the instantiation of data trusts requires data generators to have rights to portability and erasure to transfer or erase their data held by entities or within different data trusts in the ecosystem. The feasibility of data trusts is also contingent upon the jurisdiction’s articulation of data sharing principles. Further, policies that articulate purpose and data sharing standards create the right ecosystem for data trusts to further their goals by creating avenues for data sharing. Interoperability of data also ensures that data generators can exercise their rights to portability meaningfully. Similarly, ex-ante - regulatory oversight -and ex-post mechanisms - through courts - are vital to hold data trustees accountable.

ENABLERS	METRICS	INDICATORS
Data protection & Data rights	Individual data rights	• Mechanisms like portability, erasure, findability
	Protection of individual subjects’ interests	• Recourse mechanisms afforded to subjects
	Potential for delegation of data rights	• Mechanisms to assign/layer consent or exercising rights
	Collectivization of rights	• Potential for community data rights (e.g., IPR for data trusts)
Data sharing frameworks	Purpose articulation	• Guidelines/boundaries on data sharing by usage (e.g., by sector)
	Data sharing standards/infrastructure	• Regulation on standards, formats, or infrastructure such as open exchanges
	Recognition of intermediary platforms	• Mechanisms to constitute and manage data flow within intermediaries
	Differential treatment based on data type	• Established spectrum of limitations on use/sharing per data type
Fiduciary obligations	Judicial intervention	• Spectrum of judicial flexibility to affect trust functions toward beneficiary interest
	Accountability mechanisms	• Spectrum of transparency/disclosure mechanisms and regulatory oversight
	Loyalty	• Spectrum of frameworks for recognising loyalty (e.g., contractual or in-built)
	Duty of care and skill	• Spectrum of care and skill level required of fiduciaries

Figure 2.1.3 details the metrics and related indicators that have been deployed in assessing jurisdictions across the three key enablers

2.2 Selecting jurisdictions - Gating criteria and challenges

As with the establishment of analysis metrics, the selection for input of jurisdictions formed an integral part of this evaluation. Given the nascent nature of such legal landscaping, as well as that of evolving data regimes - there has been no jurisdiction that features a 'perfect' analysis, or one that completely addressed each of the enablers discussed above. In some cases, this analysis has relied on policy directives or other strategic documents and working consultations that have been indicative of prospective legislative or regulatory approaches. Thus, our gating criteria (detailed below) for the regions that feature in this analysis have been reflexive in application, based on the maturities of various data regimes.

1. Geographical representation

The selection has aimed to encapsulate perspectives and contexts of a global nature. While numerous academic initiatives have captured the movement of data governance in more developed countries, it is important to guard against systems that may end up ignoring the needs of a truly global context. Particularly for data and its ubiquitous nature, it is increasingly necessary to evaluate the direction and presence of policy in countries that may not map to the same levels of capital or technical infrastructure. The unique challenges of earlier stages are not only valuable to the assessment of feasibility of data trusts, but are important to consider when attempting to build structures of governance that seek to empower communities across borders, and of various societal structures. Thus, our eventual list features nations making up both the Global North and South.

2. Representation of various legal systems

While trust law features most foundationally through common law systems, this research has aimed to evaluate jurisdictions without a limitation to common law. A key gating criteria has been the representation of various legal systems including civil codes or mixed legal systems (that are founded on both common and civil law structures). In doing so, there have been numerous challenges to the evaluation, given that often even matching legal systems operate very distinctly in execution. In the case of fiduciary obligations as well, each region has unique frameworks and in the case of civil code, alternative pathways to instilling accountability and loyalty. Our next section chronicles some of these challenges.

3. Presence of data protection and data sharing frameworks

In order for this analysis to form a basis to future legal review, as well as be indicative of current motions in data governance - the third criteria has been a degree of discourse around data protection and data sharing. While the majority of this analysis draws from enacted legislation or prospective legislation under consultation, certain countries present valuable trends and frameworks while still functioning at the level of discussion or formulation. We found some of these to be important in this landscaping as they speak to global emerging patterns for conceptions of data trusts or intermediaries.

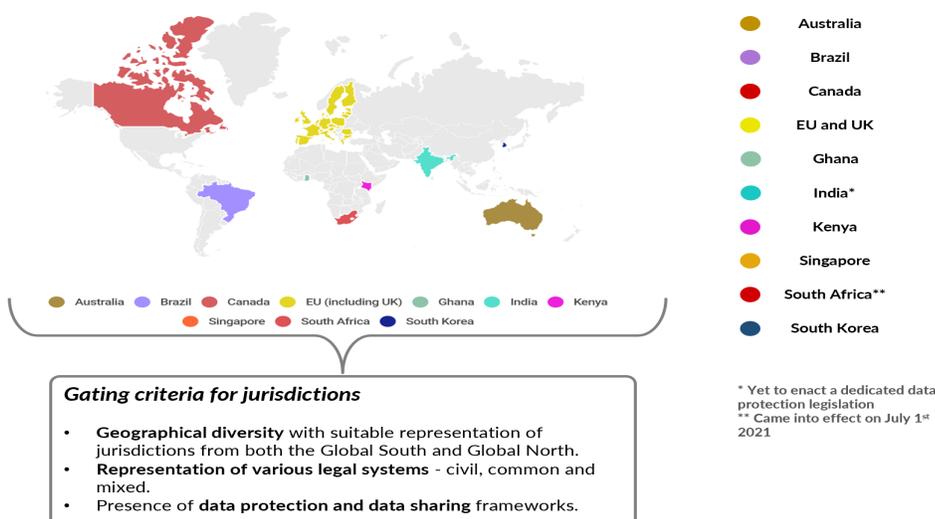


Figure 2.2.1 depicts the jurisdictions selected for this analysis, and the primary criteria applied in this selection

2.3 Chronicling decisions/challenges :

The bulk of this research deals with differences between various jurisdictions on the issue of data protection, rights and avenues for intermediaries. As with any comparative exercise, our selection of these jurisdictions and application of the analysis framework faced numerous pain points that required our approach to be iterative.

While the aim of this analysis has been to incorporate diverse legal systems, it greatly complicates the assessment of legal enablers; given that data trusts are conceptualised from common law legal trusts. They are underpinned most fundamentally by the fiduciary duty of undivided loyalty. With common law trusts recognized in very few civil law jurisdictions, our framework has included both civil legal systems that recognise trusts (Quebec and South Korea) and civil legal systems that do not (Germany and Brazil). In order to provide a landscaping on such countries, we adapted the framework and sought fiduciary-like obligations that may inspire or buttress the creation of data trusts.

The application of gating criteria for jurisdictions too, has remained reflexive and non-linear. For example, our selection needed to be cognisant of growing discourse, and not exclusively officialised legislation. In the case of Ghana, data-related legislation reflects many regulatory overlaps, and a dearth of codification around data sharing or intermediaries. However, given a strong level of political will toward data for public benefit, and a considerable shift in private sector receptivity to such regulation - it became a key focus region for our analysis. Additionally, to ensure uniformity in our comparison of legislation, our analysis has narrowed on jurisdictions that have or are moving towards federal overarching data protection regulations. This has meant the exclusion of the USA from our comparative analysis, which is currently the only OECD country that adopts a sectoral approach to regulating the use and processing of data.

The resultant framework

Based on the methodology, functions, enablers and metrics detailed above, we arrive at a working framework to evaluate the global legal landscape for enabling data trusts. Figure 2.3.1. depicts a 'preparedness' scale that has been applied to each jurisdiction based on primary analysis of policy approaches and staged. The levels illustrate the spectrum of clarity with which each metric is defined in a particular jurisdiction. The enablers are made comprehensive by the four metrics utilised under each of them.

While the levels illustrate the clarity with which each metric is defined in a particular jurisdiction, the circles on the left capture the comprehensiveness of the four metrics under each enabler. For instance, jurisdictions that recognise specific personal data rights - such as access, portability, and erasure - which are necessary for the development and operation of data trusts will place closer to the green shade of the scale, and for jurisdictions that have a weak conceptualisation of these data rights will be reflected closer to the left end i.e., red bit of the spectrum.

When interpreting this illustrated framework, it must also be noted that in capturing the recognition of these metrics, we must also account for the possibilities or restrictions that play out differently in each jurisdiction. It is, therefore, difficult to represent any of these metrics at extreme ends of the spectrum. For instance, while the GDPR recognises the right to erasure under Article 17, it is not an absolute right and has limitations as to when it can be exercised. Similarly, while some jurisdictions may not legislatively recognise certain rights, they may be represented through softer forms of laws such as policies and frameworks.

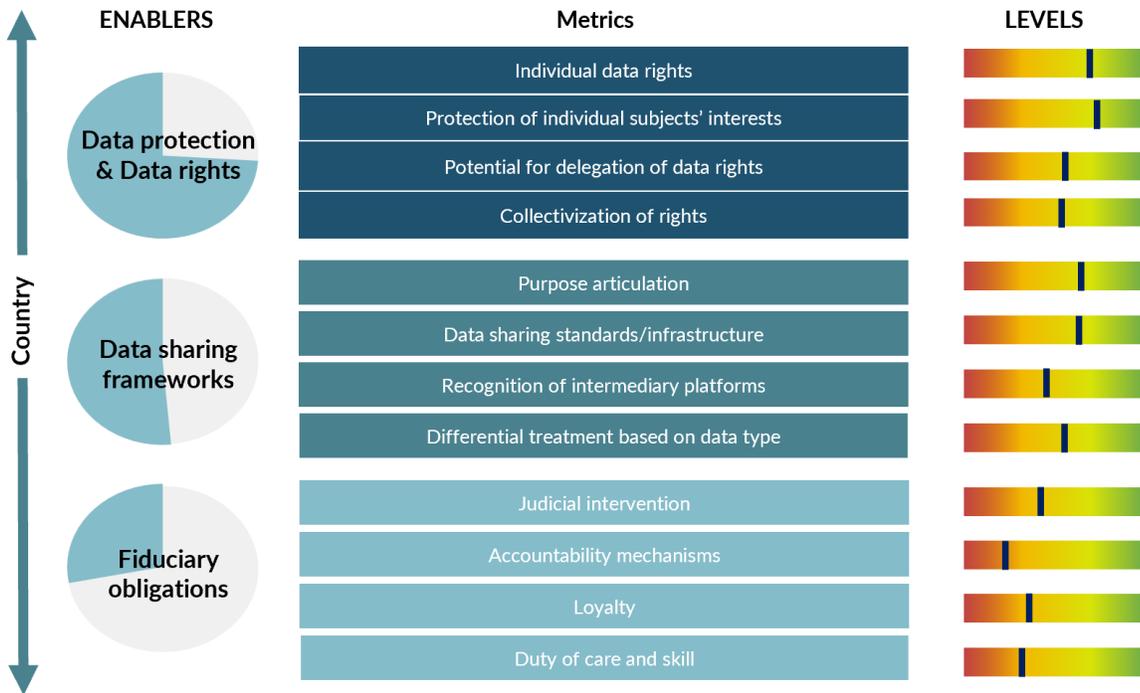


Figure 2.3.1 depicts the analysis framework that will be applied to each region (levels in this figure do not pertain to a particular jurisdiction, and are purely illustrative)

It is important to note that given the diverse nature of this analysis, and of the jurisdictions featured, this framework is not intended to be objectively linear or overly prescriptive. Instead, it provides a helpful indicative paradigm that the authors hope will be dynamic, and augmented by further research in these arenas, as data regimes make their nature and outcomes clearer over time. The deconstruction of new data governance structures, particularly human-centric structures, requires a level of deconstruction; one that this study has approached by function. Section 3 details the comparative legal analysis of each country listed, based on this framework, contextualised by the unique status and challenges of each region.

SECTORAL INSIGHTS : Snapshots from across the globe

Note: These snippets - featured here as boxes - will be scattered across the length of the report as a design break from the main content. They are currently placed together for review, but do not form their own section.

Consumer Data Right - Sectoral data sharing in Australia

Australia has taken collaborative efforts between different regulatory bodies to enable data flow across sectors. For instance, Australia's Consumer Data Right (CDR), a joint effort between the Australian Competition and Consumer Commission (ACCC), the Office of the Australian Information Commissioner (OAIC), and the Data Standards Body (DSB), is currently being rolled out to enable consumers to access and transfer their information in standardised formats. CDR aims to increase innovation and competition in the banking sector by mandating financial entities to share data. Customers have the freedom to share their banking data with competitors to compare products and services. The rollout of the CDR will take place in a phased manner, with telecommunications and the energy sector as the next identified sectors.

Consent managers as data intermediaries – Data Empowerment and Protection Architecture

In India, Niti Aayog, the government's public policy think tank, has introduced the Data Empowerment and Protection Architecture (DEPA), as a consent-based data-sharing framework that "empowers people to seamlessly and securely access their data and share it with third party institutions". It proposes the creation of 'consent managers', which are institutions that will mediate interactions between data holders and users.

In the financial sector, consent managers take the form of Account Aggregators, which are consent dashboards that allow financial entities to share data – with the user's consent – in areas such as banking, insurance, and pension. Essentially, Account Aggregators facilitate data sharing by mediating between financial institutions that hold user data with Financial Information Users who rely on such information to improve services.

Cross-sectoral data sharing in Ghana

Ghana's data collaboration initiative between Vodafone Ghana, Flowminder, and the Ghana Statistical Service (GSS) illustrates a cross-sectoral and problem-specific approach to data governance. Under the three-way agreement signed in 2019, GSS receives pseudonymised mobile data records from Vodafone Ghana, which are aggregated and analysed by Flowminder.

While the data-sharing arrangement was initially conceptualized to contain the spread of Ebola virus, it is now being used to inform policy in the government's response to the COVID-19 pandemic. For instance, the analysis of aggregated mobile data has been relied on to understand the impact of pandemic restrictions in population movements as part of the government's COVID-19 response efforts.

MyData - South Korea's sectoral approach to data reuse

Launched as part of Korea's Digital New Deal, MyData is an ambitious initiative that aims to create a common platform to share data amongst different organisations and the government to improve financial, health, and public services. The integration of individuals' data is made possible through their national identification system that issues every resident a unique identification number linked with their biometric data.

The platform will give accredited operators access to consumer information to develop innovative financial products through data analysis in the financial sector by obliging financial institutions to provide customer personal information through an application programming interface (API). The interoperability of data will allow consumers access to all their financial information in one place.

Similarly, in the health sector, the My HealthWay app provides integrated management of health information from National Health Insurance records, Health Insurance Review and Assessment Services, and the Disease Control and Prevention Agency. By 2023, the Korean Ministry of Health and Welfare aims to provide individuals with all their health records in the MyHealthWay app.

European Health Data Space

Realising the potential of data availability and reuse, the EU is pushing for common data spaces in strategic sectors to create a data sharing ecosystem. Health is one such sector where the European Commission is currently building a European Health Data Space in collaboration with the EU member states. In line with this, Europe's joint action Towards the European Health Data Space (TEHDAS) project, coordinated by the Finnish Innovation Fund Sitra and co-funded by the Health Programme of the European Union, is currently engaging with partners from different member states to advance the secondary use of health data. The project focuses on governance, data quality, and infrastructure requirements to support the secondary use of data.

Additionally, the European Commission has advanced legislative proposals such as the Data Governance Act and the Data Act that seek to overcome barriers and legal uncertainties in sharing and using data held by public and private actors. While the Data Act intends to harmonise the different regulations that pertain to the use and access of private and public sector data, the Data Governance Act seeks to create an overarching framework for data sharing through safeguards that develop trusted sharing.

SECTION 3

The following section of the report builds on the framework developed in section 2 to conduct a comparative analysis of the following eleven jurisdictions:

1. Germany
2. England and Wales
3. India
4. Canada
5. South Africa
6. South Korea
7. Australia
8. Singapore
9. Kenya
10. Brazil
11. Ghana

The comparative analysis evaluates the jurisdictions across the three enablers - data protection and rights, data-sharing frameworks, and fiduciary obligations - identified as necessary for data trusts to function. The following takeaways emerge from the comparative analysis:

- The appreciation of data rights and articulation of data sharing varies considerably across different jurisdictions. However, there is still progress in some jurisdictions without formal data rights, seen in countries like Brazil, Ghana, Canada, India, and South Africa having either amended existing laws or in the process of enacting new laws to define rights over personal data.
- The analysis found that a number of jurisdictions lacked personal data rights such as portability and erasure. This can create barriers for data trustees to represent the interests of their beneficiaries.
- Except for legislation and proposals that allow the delegation of consent in a few jurisdictions such as South Korea, Canada, and India, most personal data protection laws do not support this.
- While civil law jurisdictions like Germany and Brazil do not recognise fiduciary relationships, fiduciary-like obligations can be created contractually. Even within jurisdictions that have codified trusts, there is legal uncertainty about whether they can hold rights over data.

3.1 : Background to Comparative analysis

Having arrived at this framework, the following section carries out a comparative analysis of the selected countries to explore the varying degrees of enablers the identified jurisdictions have in place. As mentioned above, the analysis focuses on three primary legal enablers - data protection and data rights; data sharing frameworks, and fiduciary obligations. Similarly, each analysis is buttressed with the scales of preparedness based on metrics devised and elucidated earlier.

Considering the European Union's role in influencing jurisdictions outside the EU to their approach to data sharing and data regulation, the start of this comparative exercise features an overview of the EU's landscape on data rights and data sharing.

Data protection and sharing in the European Union

Personal data protection laws in the European Union are primarily covered by the GDPR (the 'Regulation'). The Regulation has been widely influential for its approach to data regulation and the rights afforded to data subjects, serving as a lodestar for numerous jurisdictions outside the EU seeking to enact data protection laws.

Chapter three of the GDPR covers the broad range of rights available to data subjects, recognising eight fundamental rights -

- a) The right to be informed
- b) The right of access
- c) The right of rectification
- d) The right to erasure
- e) The right to restrict processing
- f) The right to data portability
- g) The right to object
- h) Rights of automated decision making and profiling

In 2020, the EU released the European Data Strategy¹⁸⁰ as a policy intervention to create a single market for data sharing across different sectors. One of the outcomes of this is the proposed Data Governance Act¹⁸¹, which among other regulations, proposes to recognise a new entity - 'data intermediaries' - to manage data flow between different actors in the ecosystem. However, the draft legislation is ambiguous on the potential for delegation of the personal data rights conferred under GDPR. While it does not explicitly mention data trusts, one of the recitals in the draft legislation states that rights under the GDPR "can only be exercised by each individual and cannot be conferred or delegated to a data cooperative"¹⁸².

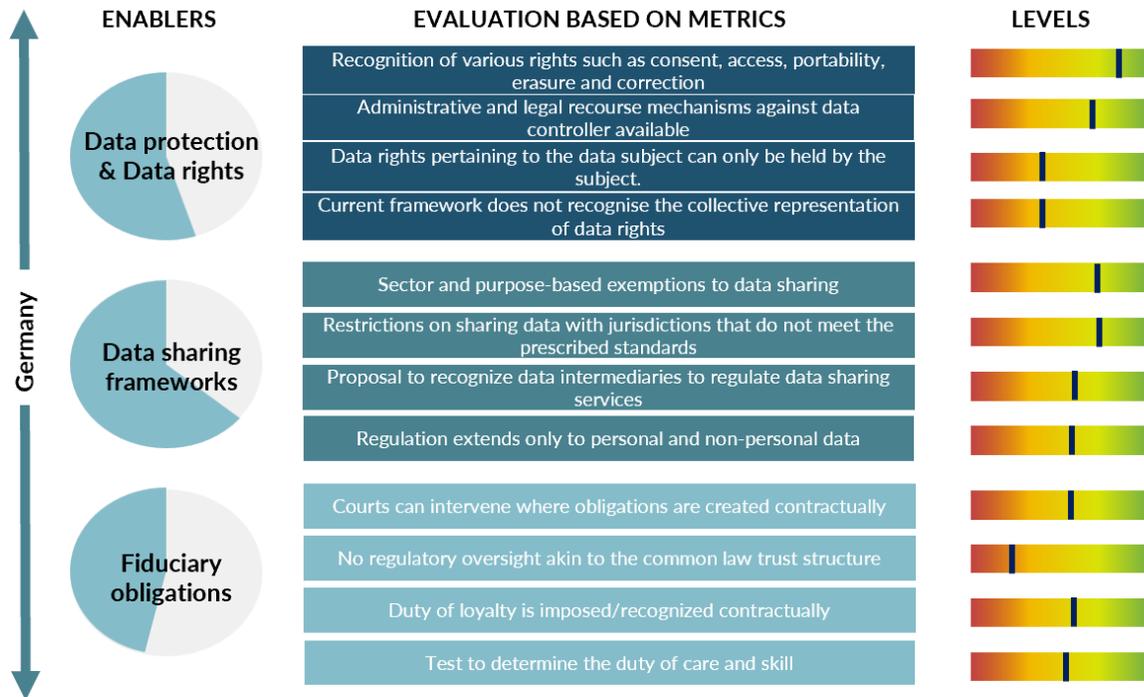
The EU has also taken steps to encourage data sharing and data re-use. One such proposal is the Data Act, which aims to incentivise horizontal data flow between organisations across sectors. The proposed legislation seeks to define the scope and contours of co-generated data rights among its other objectives. Determining the extent of such rights will enable data generators to move their data from one controller to another.

180European Commission (2021) "European data strategy" Available at: <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en>

181Shaping Europe's digital future (2021)"Data governance act" Available at: <<https://digital-strategy.ec.europa.eu/en/policies/data-governance-act>>.

182Recital 24 of the Data Governance Act. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0767&from=EN>

1. Germany



Sources:
 GDPR
 German Federal Data Protection Act (BDSG)
 European Data Strategy
 Data Act
 Data Governance Act
 Gelter and Hellinger, *Fiduciary Principles in European Civil Law Systems*

a) Data Protection and Data Rights

At the national level, Germany complemented the GDPR¹⁸³ (Regulation) with the German Federal Data Protection Act (BDSG)¹⁸⁴ and the Second Data Protection Adaptation and Implementation Act EU¹⁸⁵ to effectuate open provisions in the GDPR that are left to the member states to define. The BDSG specifies general rules and requirements for data processing applicable to the public and private sector.

While the rights to access, erasure, and portability are instrumental for individuals to move their data (or the rights over it) from one data Trust to another, at a foundational level, data Trusts need to have the authority to manage data rights. These rights extend to personal data, defined under Article 4(1) of the GDPR as any ‘information relating to an identified or identifiable natural person (‘data subject’)’. Currently, these rights can only be held by data subjects as the Regulation does not permit the transfer of data rights, nor does it recognise the collective representation or pooling of these rights. Similarly, it is unclear if there are restrictions on the transfer of rights to a third party (data trust) through assignment of consent. Consent of the data subject is one of the foundational legal bases for processing personal data under GDPR, and is (as per Article 6(1) of the Regulation) sought from the data subject for specific identified purposes.¹⁸⁶

183 General Data Protection Regulation (GDPR), 2018

Available at: <<https://gdpr-info.eu/>> [Accessed 9 May 2018].

184 Federal Data Protection Act (BDSG) of 30 June 2017. Available at: <https://www.gesetze-im-internet.de/englisch_bdsge/englisch_bdsge.html>.

185 Gabel, D (2019), “ German Bundestag passes second act on adaptation of data protection law to GDPR”, Available at <https://www.whitecase.com/publications/alert/german-bundestag-passes-second-act-adaptation-data-protection-law-gdpr>

186 Consent for broad purposes is allowed for scientific research

b) Data sharing frameworks

In recent years, after the enactment of the GDPR, the EU has been exploring ways to regulate and open data flows amongst its member states through legislation like the amended Open Data Directive¹⁸⁷ and the Regulation on the free flow of non-personal data (FFD)¹⁸⁸. In line with this, the German government announced their data strategy on January 21st, 2021 to promote data usage. The strategy prioritises four fields to enable this:

1. Creating effective and sustainable digital infrastructure
2. Innovative and responsible use of data
3. Increasing digital literacy
4. Improve the state's digital infrastructure and capacity

To this end, the German government has established a National Research Data Infrastructure to improve access to data for research.¹⁸⁹ This is also in addition to the GAIA-X¹⁹⁰, which is a federated data infrastructure that aims to create a digital ecosystem across Europe. Backed strongly by France and Europe, the move will create interoperable standards that will allow the movement of data across different silos. The initiative is also viewed as an attempt to assert Europe's digital sovereignty.¹⁹¹

c) Fiduciary obligations

As highlighted in sections above, in English law, fiduciary duties - as in the case of trusts - developed distinctly through principles of equity, imposing a stricter standard of care of one party. English law takes the view that contracts are self-interested relationships where each party pursues only their own interests. Germany, having a civil legal system, does not make this distinction in recognising fiduciary duties. These duties are, in fact, embedded contractually or through specific statutes that identify relationships that necessitate the recognition of fiduciary duties, thereby existing in a continuum and not separately.¹⁹²

One such mechanism is the *treuhand*. In a *treuhand*, the transferor transfers their assets (and its ownership) to the trustee.¹⁹³ However, while the ownership rests with the trustee, the trustee is bound by 'mandate', a type of agency relationship. Mandate is a legal relationship that permits one party to represent or act on behalf of the other.¹⁹⁴ It remains unclear whether data trusts can be recognised in this relationship.

Moreover, courts can only intervene only where such obligations arise contractually or through the operation of these specific statutes. However, even then, courts in civil legal systems may not have the same flexibility to evaluate decision-making of trustees in polycentric aspects that arise in the administration of trusts.

187 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information PE/28/2019/REV/1 <https://eur-lex.europa.eu/eli/dir/2019/1024/oj>

188 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union PE/53/2018/REV/1 Available at: <http://data.europa.eu/eli/reg/2018/1807/oj>

189 National Research Data Infrastructure, 2021 Available at: https://www.dfg.de/en/research_funding/programmes/nfdi/index.html.

190 See, <https://www.data-infrastructure.eu/GAIA-X/Navigation/EN/Home/home.html>.

191 Delcker, J. and Heikkilä, M (2020), POLITICO, " Germany, France launch Gaia-X platform in bid for 'tech sovereignty.' ". Available at <https://www.politico.eu/article/germany-france-gaia-x-cloud-platform-eu-tech-sovereignty/>.

192 Gelter, M and Helleringer, G (2018), Oxford Handbook of Fiduciary Law, "Fiduciary Principles in European Civil Law Systems", Available at SSRN: <https://ssrn.com/abstract=3142202>

193 Gvelesiani, Irina (2016), CES Working Papers, "EU Policies Regarding the Development of Trust-Like Devices - Recent Challenges, Achievements, Prospects and Terminological Insights

194 Gelter and Helleringer (n. 51).

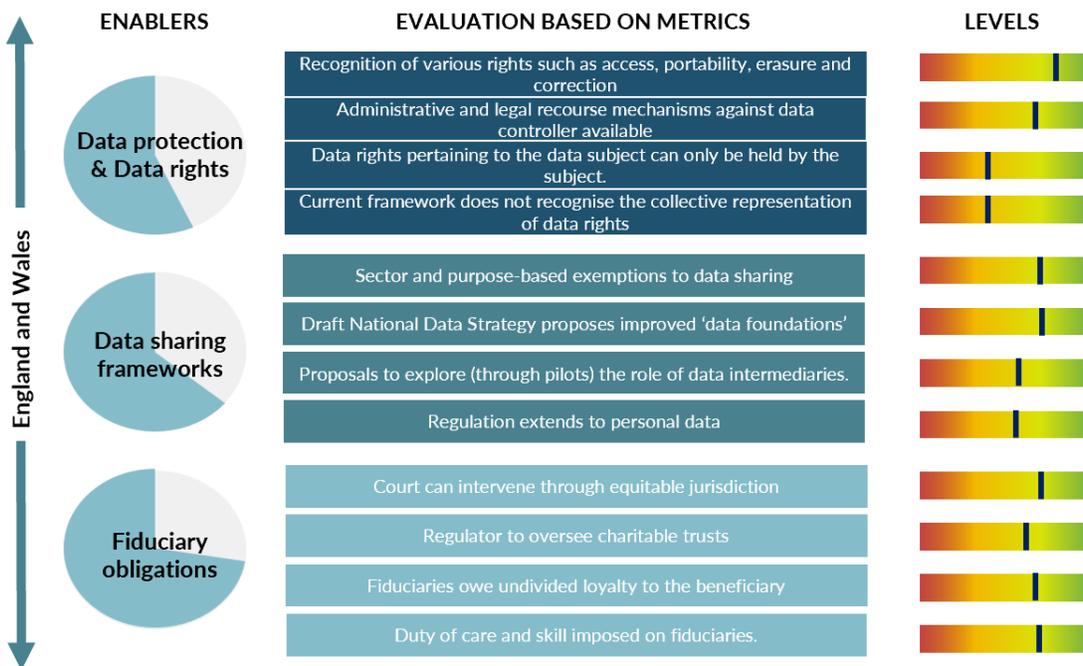
Key takeaways

From our exploration of Germany’s legal landscape, it becomes clear that Europe’s approach towards recognising rights over personal data and articulating data sharing is robust compared to other jurisdictions. With efforts underway to develop interoperable standards for data spaces across Europe, in the health sector, for instance, data trusts have the potential to tap into these infrastructures to represent the collective interests of beneficiaries. However, GDPR’s current conceptualisation of rights over personal data does not acknowledge the rights to mandate individual rights over data, which greatly hinders the possibility of setting up data trust-like initiatives. .

While Germany does not distinguish fiduciary duties in the same way as English law, it does recognise similar obligations contractually, allowing courts to intervene in disputes arising in the performance of these obligations. However, reliance on contractual obligations can create difficulties for representing rights, which requires specific contractual relationships with each individual wishing to participate in a data trust. Similarly, the absence of a legal trust framework requires either the adoption of existing structures such as companies or associations, or the recognition of a new class of intermediaries that can carry out the functions of a data trust.

The Opinion of Data Ethics Commission recognises great potential in data management and data trust schemes to empower individuals to take control over their personal data. The commission also recognises the “Right to digital self determination” and is against the idea of data ownership and believes that contribution to generation of data must lead to “ data specific rights of co-determination and participation” which is dependent on several factors. The Commission also recommends clarification of S.311 of the German Civil Code to include quasi-contractual duties which are fiduciary in nature for data controllers. These recommendations show that Germany is attempting to codify fiduciary obligations and adopting data trust-like schemes.

2. England and Wales



Sources:
 Data Protection Act 2018
 National Data Strategy
 The Charities Act 2006
 Unlocking the value of data: Exploring the role of data intermediaries - CDEI Report

a) Data Protection and Data Rights

Post-Brexit, the UK was categorised as a third country by the EU under the GDPR¹⁹⁵. However, the free flow of information continues to occur through a decision adopted by the EU on the adequacy of protection of personal data by the United Kingdom¹⁹⁶. The UK Data Protection Act 2018¹⁹⁷ was legislated to adopt the EU GDPR, with minor procedural and cosmetic amendments. It, therefore, recognises the same rights for data subjects - as discussed above - set out under the EU GDPR¹⁹⁸. Unless data is anonymised completely, data trusts in both the EU and the UK will have to ensure that processing is carried under one of the six lawful bases for processing data.

b) Data sharing frameworks

In 2020, the UK government published the **National Data Strategy**¹⁹⁹ to explore opportunities and avenues for data use. In line with this, the government identified four pillars - foundations, skills, availability and responsibility - that align to its actions or 'missions'. The five missions are to: unlock the value of data across the economy; secure a pro-growth and trusted data regime; transform government's use of data; ensure the security and resilience of its data infrastructure, and engage in the international flow of data.²⁰⁰

To advance the aims set out in the National Data Strategy, the Centre for Data Ethics and Innovation published an independent report, commissioned by the Department for Digital Culture, Media, and Sport (DCMS), to explore ways in which data intermediaries could support data sharing.²⁰¹ Identifying existing organisations that play the role of data intermediaries in the current digital economy, the report suggests ways in which intermediaries can enhance the value of publicly and privately available data.

On 10 September 2021, as part of one of its missions to "secure a pro-growth and trusted data regime", the government launched a consultation to reform its data protection laws.²⁰² The proposal seeks to remove barriers in the current General Data Protection Regulation (UK GDPR) to support "vibrant competition and innovation to drive economic growth".²⁰³ Equally, the Department for Digital, Culture, Media and Sport (DCMS) has proposed broadening the remit of the Information Commissioner's Office to "champion sectors and businesses that are using personal data in new, innovative and responsible ways to benefit people's lives" in areas such as healthcare and financial services²⁰⁴.

c) Fiduciary Obligations

Fiduciary principles in English common law can be traced back to the courts of equity in Medieval England which typically relied on notions of undivided loyalty and good faith to recognise ownership of property held in trusts. Until the 19th century, remedies from common law and equity were distinctly applicable. In 1873, the Parliament passed the Judicature Act that merged the Court of Chancery and Court of Law to the High Court, which applies either principle as applicable²⁰⁵. Therefore, the law of trusts and fiduciary was purely a creation of the Court of Chancery institutionalised into common law.

Trusts are typified by a fiduciary relationship between the trustee and the trust's beneficiaries. Unlike other fiduciary relationships - a doctor and a patient or a director and the company, for instance - trustees are bound by stricter standards of loyalty and a duty of care/prudence. Trustees who fail to uphold these

195 See <https://ico.org.uk/media/for-organisations/documents/brexit/2617110/information-rights-and-brexit-faqs-v2_3.pdf>.

196 See <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/>>.

197 Data Protection Act, 2018. Available at: <https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf>.

198 *ibid*.

199 See <<https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy>>

200 *ibid*.

201 See <https://legislative.gov.in/sites/default/files/A1882-02.pdf>

202 See <<https://www.gov.uk/government/consultations/data-a-new-direction>>.

203 *ibid*.

204 Department for Digital, Culture, Media and Sport(2021),"UK launches data reform to boost innovation, economic growth and protect the public "Available at: <<https://www.wired-gov.net/wg/news.nsf/articles/UK+launches+data+reform+to+boost+innovation+economic+growth+and+protect+the+public+13092021101010?open>>.

205 The Judicature Acts of 1873 and 1875. Available at: <<https://www.parliament.uk/about/living-heritage/transformingsociety/laworder/court/overview/judicatureacts/>>.

principles can be removed from office, surcharged, or enforced to disgorge profits. This counteracts potential ex-post disputes, which often arise in agency relationships where agents engage in self-dealing.

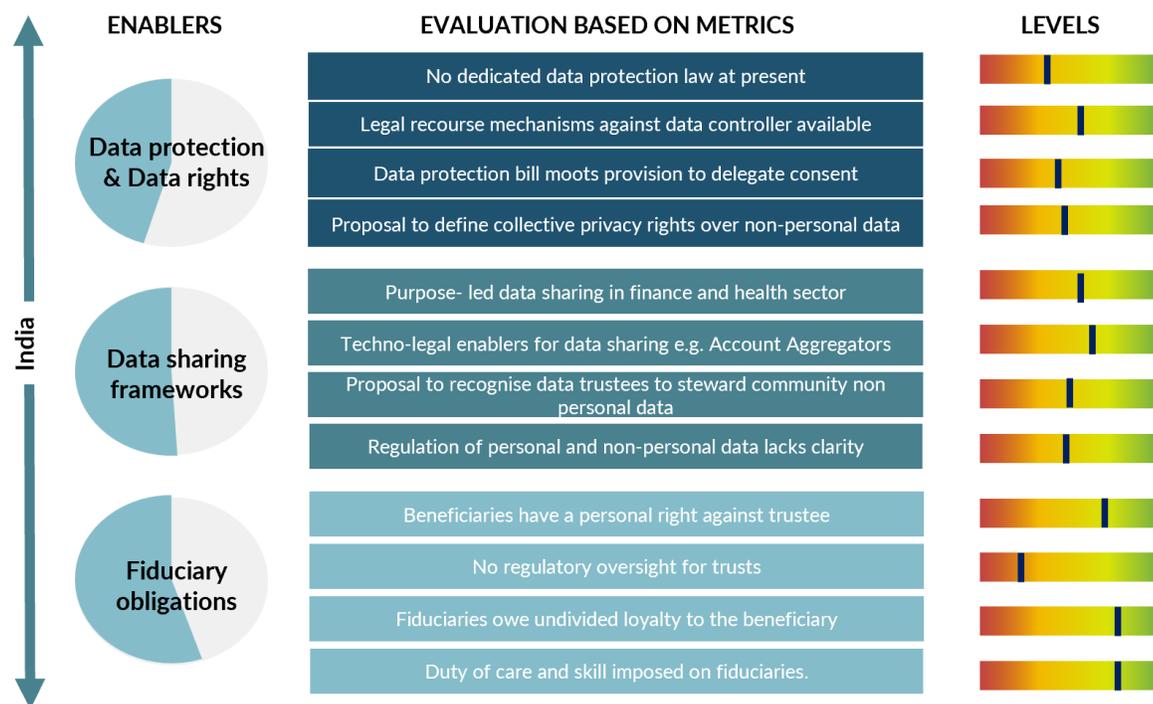
Key takeaways

Naturally, trusts' institutional and legal origins in England and Wales make it the most suitable for instantiating data trusts through trust law. Additionally, the influence of GDPR in the UK's recognition of rights of access, portability, and erasure creates a suitable ecosystem for developing a plurality of data trusts.

However, given the different rules that can apply to data, there needs to be legislative certainty across various sectors for data trusts to access and use data meaningfully. For instance, the proposed Data Act in the European Union aims to bring legal certainty by harmonising the different regulations – e.g., database rights, trade secrets – that can affect the access and use of data.

Although trusts traditionally lack regulatory oversight, charitable trusts in the UK fall within the remit of the Charity Commission. Given current attempts to pilot data trusts in the UK, the scope and requirements for ex-ante regulation for the functioning of data trusts is a potential safeguard mechanism worth considering.

3. India



Sources:
 IT Act, 2000
 Personal Data Protection Bill 2019
 Report on Non Personal Data Framework
 Data Empowerment and Protection Architecture
 Indian Trusts Act 1882

a) Data protection and Data Rights

While India recognises the fundamental right to privacy within Article 21²⁰⁶ (right to life and liberty), it is still yet to enact dedicated data protection legislation. Currently, data protection is regulated by the Information

206 Article 21 of the Constitution of India

Technology Act, 2000 (IT Act), and the rules under it²⁰⁷. For instance, the distinction between personal data and sensitive personal data is made in the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules framed under the IT Act (SPDI Rules)²⁰⁸. Section 43A of the IT Act grants individuals the right to claim compensation for wrongful loss if body corporates do not have reasonable security measures in place. SPDI rules define personal information as any information that relates to a natural person which, either directly or indirectly, in combination with other available or likely available information, may identify that person²⁰⁹.

While the IT Act's conception of data protection is quite limited in scope, only recognising consent, access, and correction rights, the proposed Personal Data Protection Bill (PDPB)²¹⁰, drafted in the backdrop of the landmark judgement that recognised the right to privacy²¹¹, extends additional rights like the right to erasure and portability. The PDP Bill also envisages giving data principals the right to delegate the exercise of their agency (provide or withdraw consent) to a new category of data fiduciaries termed as consent managers²¹².

Concurrently, the Indian Government has also published a report on the regulation of non-personal data. It proposes collective privacy rights over non-personal data in contrast to the framing of rights over personal data, where the individual is the focal point.

b) Data sharing frameworks

In recent years, NITI Aayog, the Indian government's public policy think tank, has mooted techno-legal approaches to enhance access to and sharing of data. The proposed Data Empowerment and Protection Architecture (DEPA)²¹³, for instance, is public-private collaboration that builds on the concept of consent managers to create a platform that allows data transfers from one entity to another. The finance sector and health sector have already made some inroads through the adoption of 'account aggregators' and the National Health Stack²¹⁴.

At the same time, there are proposals to create interoperable sharing infrastructure for non-personal data.²¹⁵ The report on the Non-Personal Data Governance Framework (the "NPDR") report recognises beneficial interests over community data. The committee identifies five key principles to ascertain community rights over data: (i) a community's right over resources associated collectively with it; (ii) consent of the community for use of such resources; (iii) benefit sharing with the community; (iv) transparency in recording community resources to prevent misuse and enable easy access of the legitimate kind; and (v) community's participation in governance of community resources.²¹⁶ The NPDR also recommends the creation of 'data trustees' as intermediaries to exercise rights on behalf of the group/community. The committee sources this community right from Article 39(b) and (c) of the Indian Constitution (Directive Principles of State Policy)²¹⁷ which stipulates that the ownership and control of resources ought to be distributed to serve the common good and to prevent the concentration of wealth.

207 The Information Technology Act 2000,

see https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

208 *ibid.*

209 *ibid.*

210 Personal Data Protection Bill 2019,

see http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

211 Justice K.S. Puttaswamy vs. Union of India (2017) 10 SCC 1, AIR 2017 SC 4161

See https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

212 Personal Data Protection Bill, 2019

213 NITI Aayog (2020), "Data Empowerment and Protection Architecture." Available at: <<https://www.niti.gov.in/sites/default/files/2020-09/DEPA-Book.pdf>>.

214 NITI Aayog (2018), "National Health Stack Strategy and Approach." Available at: <https://ndhm.gov.in/publications/NHS_Strategy_and_Approach>.

215 The Ministry of Electronics & Information Technology (2020), "Report by the Committee of Experts on Non-Personal Data Governance Framework"

see https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf

216 The Ministry of Electronics & Information Technology (2020), "Report by the Committee of Experts on Non-Personal Data Governance Framework"

See https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf

217 Article 39(b) and (c) of the Constitution of India

c) Fiduciary obligations

Fiduciary obligations concerning trust law in India are primarily codified in the Indian Trusts Act 1882 ('Trusts Act')²¹⁸. Fiduciary obligations can also be located in other relationships, such as an agent to a principal and directors to their company. In the Supreme Court case of the *Reserve Bank of India v. Jayantilal N. Mistry*²¹⁹, the court observed that fiduciaries owe "undivided loyalty to the beneficiary, not to place himself in a position where his duty towards one person conflicts with a duty that he owes to another customer".

The Trusts Act pertains to private trusts, which are essentially trusts with clearly identified beneficiaries. Public trusts must be created for charitable, educational, religious or scientific purposes and be for the benefit of a specific class or the general public. The Trusts Act recognises obligations such as loyalty, care, and prudence through various provisions that impose duties and liabilities on trustees. For instance, section 14 of the Act requires the trustee to ensure that the title of the trust property is not dealt with (self dealing or otherwise) in a manner that adversely affects the beneficiary.²²⁰ Similarly, section 15 mandates the trustee to deal with the trust property "a man of ordinary prudence would deal with such property if it were his own".²²¹

However, the subject-matter of a trust must be property that is transferable to the trust.²²² The development of case law on the scope of the subject-matter is limited. It is, therefore, unclear, data (or the rights over it) can constitute as the subject matter of trusts under Indian law. Moreover, unlike in English law, the Indian Trusts Act does not recognise the concept of dual-ownership. Beneficiaries only have a beneficial interest against the trustee, who is the sole owner of the trust property.

Key takeaways

Although restricted to non-personal data, India's Non-Personal Data Governance Framework report offers a unique articulation of data trustees to manage community rights over data. The report proposes data trustees as intermediaries representing and protecting the community's interests by recognising collective rights over privacy. However, the current framework does not identify procedural safeguards or mechanisms that can hold trustees accountable.

While India has codified trusts and trustee's fiduciary responsibilities, the feasibility for legal trusts to hold data rights as the subject matter lacks legal certainty. Moreover, in the absence of dedicated data protection legislation, India's recognition of individual rights over personal data remains weak, further restricting the possibility of data trusts' to act as intermediaries.

²¹⁸The Indian Trusts Act 1882, see <https://legislative.gov.in/sites/default/files/A1882-02.pdf>

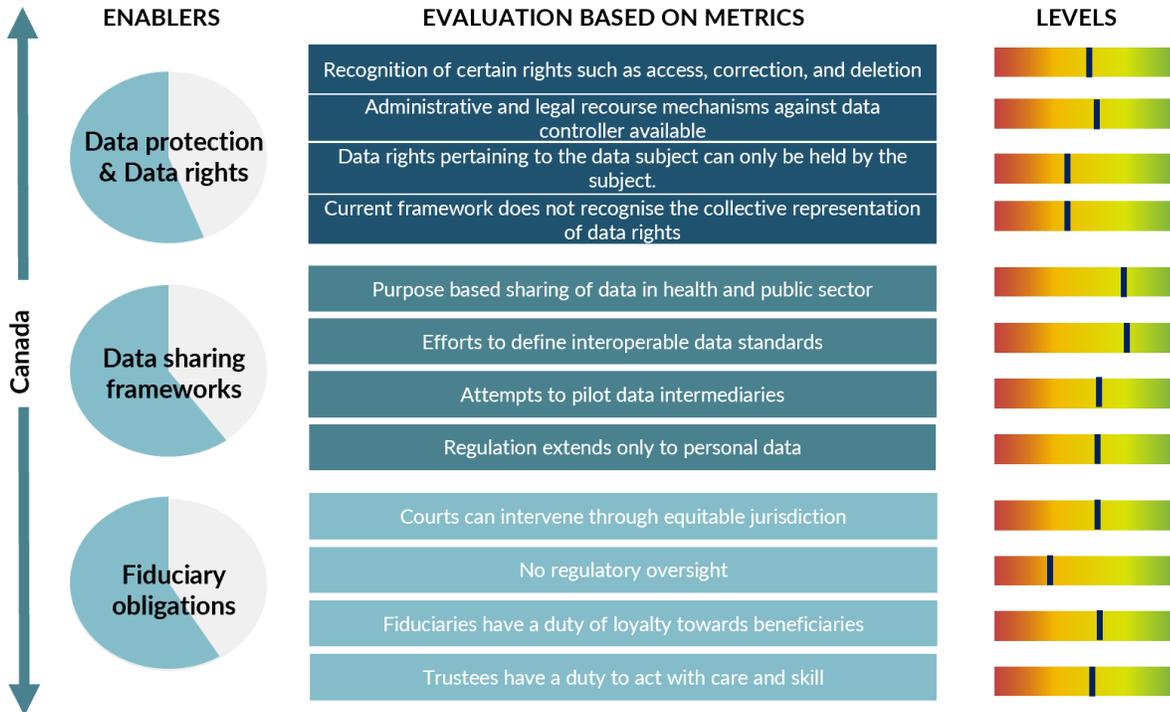
²¹⁹ RBI vs Jayantilal Mistry https://main.sci.gov.in/supremecourt/2019/31871/31871_2019_37_1503_27802_Judgement_28-Apr-2021.pdf

²²⁰ Section 13 of the Indian Trusts Act 1882, see <https://legislative.gov.in/sites/default/files/A1882-02.pdf>

²²¹ Section 15 of the Indian Trusts Act 1882, see <https://legislative.gov.in/sites/default/files/A1882-02.pdf>

²²² Section 8 of the Indian Trusts Act 1882, see <https://legislative.gov.in/sites/default/files/A1882-02.pdf>

4. Canada



Sources:
 PIPEDA 2000
 Privacy Act
 Digital Charter Implementation Act 2020
 Consumer Privacy Protection Act
 Canada Data Strategy
 Canadian Data Governance Standardisation Collaborative

a) Data protection and Data rights

Data protection in Canada is governed by a mix of general and sector-specific legislation, both at a federal and provincial level.²²³ At the federal level, Personal Information Protection and Electronic Documents Act 2000 (PIPEDA)²²⁴ regulates the private organisations' use of personal data and the Privacy Act²²⁵ governs the public sector's use of personal data. The legislation was amended several times since it was first enacted in 2000, the most significant amendment being the Digital Privacy Act²²⁶ in 2015 which expanded the Information Commissioner's powers and introduced mandatory breach notification. Under the current framework, individuals have limited right to access and seek correction of their personal data.²²⁷

On November 17, 2020, the federal government tabled the Digital Charter Implementation Act²²⁸ to overhaul the current privacy legislation. The Act introduces substantial changes to the current privacy framework, including the new Consumer Privacy Protection Act (CPPA), which seeks to regulate privacy laws in the

223 Quebec, British Columbia, and Alberta have their own provincial statutes.

224 Office of the Privacy Commissioner of Canada, PIPEDA legislation and related regulations - Office of the Privacy Commissioner of Canada. Available at: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/.

225 Canadian Ministry of Justice, Privacy Act. Available at: <https://laws-lois.justice.gc.ca/PDF/P-21.pdf> [Accessed 23 September 2021].

226 Digital Privacy Act 2015, see https://laws-lois.justice.gc.ca/eng/annualstatutes/2015_32/page-1.html

227 Schedule 1 Principle 9 of PIPEDA

228 Digital Charter Implementation Act 2020, see https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html

private sector²²⁹. In addition to the existing rights to access and correction, the Bill introduces rights of erasure and portability.

b) Data sharing frameworks

At the governmental level, machine readable public sector data is made available for reuse under its Open Government Initiative.²³⁰ Only data that is safe, legally permissible, and not identifiable to individuals is shared. Departments of the government also have a sectoral approach to data sharing. The Pan-Canadian Health Data Strategy, for instance, empowers the Corporate Services Branch (CSB) and the Business Renewal and Enterprise Architecture Directorate (BREAD) “to effectively use data as an asset to provide credible information, reliable advice and quality services”²³¹.

Additionally there have been efforts at a cross-sectoral level to increase data sharing by improving interoperability of data. For instance, in 2019, the Standards Council of Canada constituted the Canadian Data Governance Standardization Collaborative (DGSC), comprising over 200 members of stakeholders from various industries, civil society, and academia to streamline data standardization practices by keeping all stakeholders in mind²³².

c) Fiduciary obligations

Canada’s influence of both civil and common law origins makes it a unique jurisdiction of study. While common law in Canada extends fiduciary duties beyond trustee and beneficiary relationships, civil law in Quebec does not recognise these fiduciary relationships. Like many civil law jurisdictions, the Quebec Civil Code codifies obligations of good faith and loyalty within contractual relationships.²³³

Except in Quebec, which has civil law trusts, provinces of Canada have common law origins of trusts. And in contrast to common law trusts, which are based on the principle of ownership with obligation owed by the trustees towards its beneficiaries, trusts in Quebec are concerned with the advancement of a purpose through the administration of appropriated property.²³⁴ The underlying principle of civil trusts is that the question of ownership does not arise; trusts and its administration is defined by the purpose it seeks to achieve.²³⁵ The settlor determines the purpose (in the case of data trusts, individuals, or organizations seeking to share their data).²³⁶ In both civil and common law trusts, trustees owe fiduciary duties of diligence, prudence, and loyalty. Moreover, settlers, beneficiaries, and ‘interested persons of interest’ have the right to institute proceedings against the trustee if trustees fail to comply with their obligations.²³⁷

229Consumer Privacy Protection Act (CPPA), 2020.

See <https://www.parl.ca/LegisInfo/BillDetails.aspx?Language=e&Mode=1&billId=10950130>

230 Government of Canada, Open Government Initiative, see <https://open.canada.ca/en/open-data-principles>

231 Government of Canada, Pan-Canadian Health Data Strategy, see <https://www.canada.ca/en/public-health/programs/pan-canadian-health-data-strategy.html>

232 Standards Council of Canada (SCC), Canadian Data Governance Standardization Collaborative (DGSC), see <https://www.scc.ca/en/flagships/data-governance>

233 See Article 1375 and Article 322 (in the case of directors) of the Quebec Civil Code <http://legisquebec.gouv.qc.ca/en/showdoc/cs/ccq-1991>

234 Article 915, Civil Code of Quebec

235 Mettarlin, D.N(1975), McGill Law Journal, The Quebec trust and the civil law.”

236“Sophie Hulin A, “ How can civil jurisdictions support data trusts? The Quebec Example “ Available at <https://datatrusters.uk/blogs/how-can-civil-law-jurisdictions-support-data-trusts-the-quebec-example>

237 Article 1290, Civil Code of Quebec.

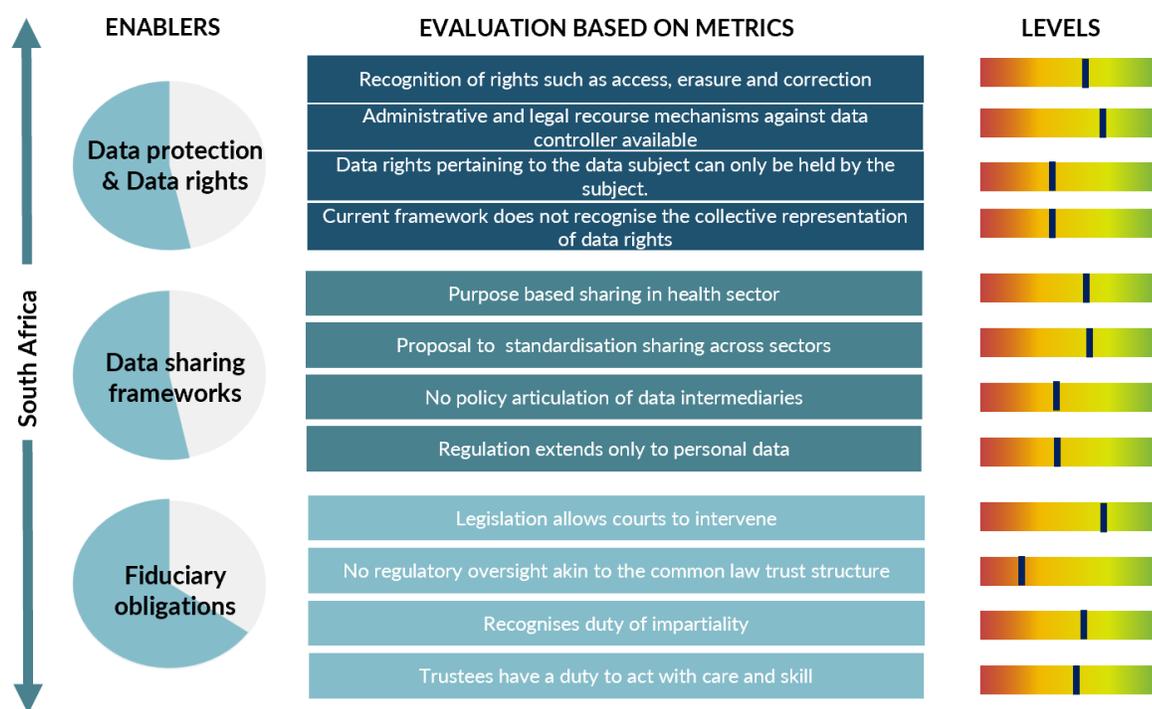
Key takeaways

In comparison with other jurisdictions, Canada's recognition of trusts is unique, with the presence of both civil and common law trusts. The Civil Code of Quebec offers flexibility to create data trusts for a wide range of purposes by recognising the creation of trusts for commercial and non-commercial purposes. Furthermore, the absence of ownership requirements for Quebec civil trusts means that the question of ownership of data to represent rights over data trusts does not arise.

However, at present, Canadian laws do not confer personal data rights of portability and erasure. The absence of these rights poses challenges to sustain an ecosystem of data trusts that can meaningfully make decisions on the personal data of individuals held by entities. Although Quebec's recently adopted Bill-64 recognises the right to portability, it will only come into force in 2024. Similarly, the proposed Digital Charter also moots recognizing the right to portability and a limited right of erasure.

From interactions with experts, we observed a marked push at an ecosystem level from both the public and private sector to explore different data stewardship models in Canada. Aside from Ontario's attempts to create urban data trusts, the potential for data trusts as a form of data stewardship is being investigated by public and private actors across Canada.²³⁸

5. South Africa



Sources:

- Protection of Personal Information Act (POPIA) 2013
- National Digital Health Strategy
- National Data and Cloud Policy
- Trust Property Control Act, 1988.

238 See, <https://tiess.ca/wp-content/uploads/2021/03/Data-Trusts-In-Quebec-Civil-Law-Synthesis-2.pdf>
<https://marsdd.gitbook.io/datatrust/trusts/what-is-a-civic-digital-trust>
https://hello.elementai.com/rs/024-OAQ-547/images/Data_Trusts_EN_201914.pdf
<https://datatrusts.uk/blogs/how-can-civil-law-jurisdictions-support-data-trusts-the-quebec-example>

a) Data protection and data rights

Like India, the right to privacy as a fundamental right is constitutionally recognised within the South African Constitution's Bill of Rights²³⁹. However, it was only on July 1st 2020, that the country's data protection legislation, Protection of Personal Information Act 2013 (POPIA), came into effect²⁴⁰. The POPIA grants individuals the right to access and request correction or erasure of their personal data. Additionally, individuals also have the right not to be subject to decisions that are made solely on the basis of automated processing of their personal information.²⁴¹

The legislation also contains provisions that allow individuals to approach the data protection regulator or courts where individuals feel that there has been an interference with the protection of their personal data.

b) Data sharing frameworks

In tandem with its data protection law reform, the South African government has also published the Draft National Data and Cloud Policy as a bid "to realise the socio-economic value of data through the alignment of existing policies, legislation and regulation"²⁴². The policy applies to the public and private sector, and makes recommendations on various issues, ranging from access to data, cross-border data transfers, competition in the digital economy, and digital infrastructure. Seen as a response to the growing concerns of concentration of data under the control of tech corporations²⁴³, through data localisation proposals, the policy emphasizes asserting sovereignty over data generated within the country.

Equally, there are also sector-specific approaches being taken to promote data sharing. One of the interventions of the National Digital Health Strategy for South Africa²⁴⁴ is to enhance data use in the health sector through data sharing agreements with third party health information systems. The digital health strategy also prioritises the creation of an "integrated platform and architecture for health sector information systems" that will provide interoperable connection with patient information systems.

South Africa follows a mixed legal system, with Roman-Dutch and English law origins, and is evidenced in their recognition of trusts.²⁴⁵ However, like with the Indian conception, South African law does not recognise English law's dual ownership of the trust property.²⁴⁶ Therefore, trust law was, therefore, codified through the Trust Property Control Act 1988 (TPCA)²⁴⁷, recognising trusts where the ownership either lies with the trustee (English influence) or where the trustee manages assets that are bequeathed to the beneficiaries (Dutch influence).²⁴⁸

The TPCA imposes duties of care, skill and diligence, trustees duties of loyalty are specified in the statute. However, the principles governing fiduciary actions are derived from equitable principles of English law, and the duty of impartiality²⁴⁹ is implicit in the responsibilities of a trustee.²⁵⁰ The TPCA grants courts discretion

239 Section 14 of the Constitution of the Republic of South Africa, see <https://www.gov.za/documents/constitution/chapter-2-bill-rights#14>

240 Protection of Personal Information Act (POPIA) 2013, see <https://popia.co.za/category/popia/>

241 *ibid*.

242 Section 3(5) of the Electronic Communications Act, 2005.

See https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf

243 Spuy, A. (2020) "Should we nationalise data? In conversation with Ulises Mejias" Available at: <<https://blogs.lse.ac.uk/medialse/2020/04/07/should-we-nationalise-data/>>.

244 Department of Health, South Africa. National Digital Health Strategy. see <http://www.health.gov.za/wp-content/uploads/2020/11/national-digital-strategy-for-south-africa-2019-2024-b.pdf>

245 Du Toit, F. (2013), Cambridge University Press, "Jurisprudential milestones in the development of trust law in South Africa's mixed legal system", doi:10.1017/CBO9781139505994.012

246 *Braun and Another v Botha and Another* (263/82) [1984] ZASCA 19

247 Trust Property Control Act, 1988.

See https://www.gov.za/sites/default/files/gcis_document/201505/act-57-1988_0.pdf

248 Clarry, D (2014), *The International and Comparative Law Quarterly*, "Fiduciary Ownership and Trusts in a comparative perspective", <https://doi.org/10.1017/S0020589314000463>

249 Rahman, L, University of the Western Cape, "Defining the concept 'Fiduciary Duty' in the South African Law of Trusts", Available at https://etd.uwc.ac.za/bitstream/handle/11394/2144/Rahman_LLM_2006.pdf?sequence=1

250 *Phillips v Fieldstone Africa (Pty)* 2004 (3) SA 465 (SCA)

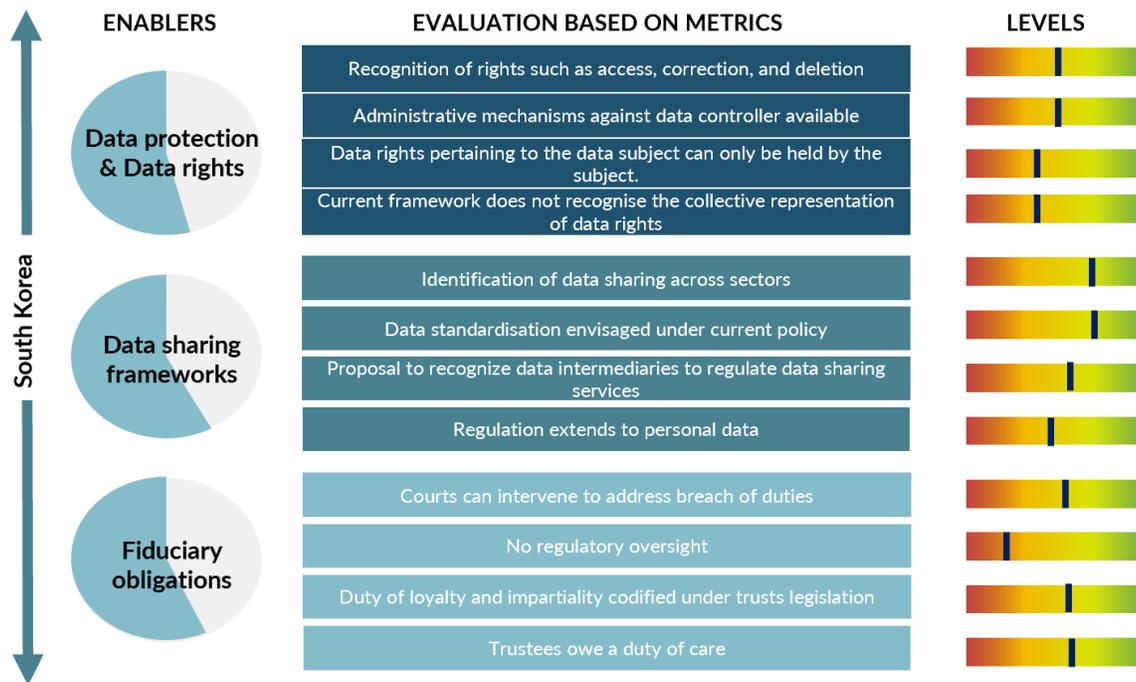
to intervene to vary trust provisions, where the courts of the opinion that the provisions can “prejudice the interests of the beneficiaries”.²⁵¹

Key takeaways

While South Africa’s Trust Property Control Act presents flexibility by allowing the creation of trusts where ownership of property lies with the beneficiary, there are key challenges that arise in the development of data trusts.

First, given the recency in enacting regulations over the use of personal data, the scope and applicability of rights over personal data in South Africa are still underexplored. The absence of data portability rights and the limited recognition of the right to erasure, for instance, could create barriers for trustees to advance the interests of the beneficiaries. Second, the development of data trusts requires clarity on whether POPIA allows trustees as third parties to manage individual’s rights over their personal data.

6. South Korea



Sources:
 Personal Information Protection Act, 2011
 Network Act
 Digital New Deal
 Trust Act 2011

a) Data protection and Data rights

As one of the most connected jurisdictions, South Korea (Korea) was quite early in legislating comprehensive regulations on the use of data. The regulation of personal data is governed by the Personal Information Protection Act 2011 (PIPA)²⁵². The legislation extends to both public and private actors. In addition to the

251 Section 13 of the Trust Property Control Act

252 Personal Information Protection Act, 2011.

See https://www.privacy.go.kr/eng/laws_view.do?nttld=8186&imgNo=3

PIPA, there are sector specific laws around health, finance, and e-commerce that govern the use and sharing of information such as the Act on Promotion of Information and Communications Network Utilization and Information Protection 2001 ('ICNA'; also known as Network Act), and the Credit Information Use and Protection Act 2008 ('the Credit Information Act'). While the PIPA grants individuals with data rights such as access, correction, erasure, it currently does not recognise data portability rights.

In 2020, the National Assembly made amendments to the three major privacy legislation - the PIPA, the ICNA and the Credit Information Act - to streamline the application of data protection laws²⁵³. While ICNA operates as a specialised legislation, provisions of the ICNA pertaining to personal information were subsumed into the PIPA.

Interestingly, Article 38 of PIPA allows individuals to authorise representatives to file requests to access, correct, erase or suspend data processing on behalf of the individual.²⁵⁴

b) Data sharing frameworks

Policy makers in Korea were comparatively early in identifying data sharing strategies, with most government processes digitised during the previous decade. In June 2020, through a major policy initiative, called the Digital New Deal, the Korean government announced several measures to strengthen its digital infrastructure and cloud computing and increase the convergence between 5G and AI²⁵⁵. One of the measures is the 'Data Dam' project, which includes various methods for data standardisation, processing, and utilisation²⁵⁶. The Digital Deal also proposes to build new platforms under the 'MyData' initiative. These platforms aim to support citizens and provide services across healthcare, public services, finance, and transportation.

Korea, through its data protection laws, however, attempts to implement data localisation practices. For instance, transferring personal information abroad requires data controllers to notify and obtain consent from the data subject. Additionally, restrictions are imposed on transferring information to organisations based in jurisdictions that have restricted the transfer of personal information abroad.

c) Fiduciary obligations

Korea codified trusts through the Korean Trust Act 1961²⁵⁷ In 2009, after extensive deliberations by the trust law reform committee, the 1961 legislation was replaced by the Trust Act 2011²⁵⁸ to govern private trusts. It defines trusts as a legal relationship where the trustor "transfers a specific piece of property (including part of business or an intellectual property right) to a person who accepts the trust,... and requires the trustee to manage, dispose of, operate, or develop such property or engage in other necessary conduct to fulfill the purpose of the trust, for the benefit of a specific person or for a specific purpose, based on a confidence relation between the trustor and the trustee"²⁵⁹. The legislation adopts a broad framing of property which could allow personal rights to form the subject matter of trusts.

Chapter IV of the Trust Act codifies various duties of a trustee such as the duty of care, the duty of loyalty, and the duty of impartiality. Moreover, a trustee should not benefit from their position or put themselves in a position having a conflict of interest. Beneficiaries have personal rights against their trustees.²⁶⁰ Under article 43(3) of the Trust Act, if the trustee is found to be in breach of their duties, beneficiaries can disgorge any benefits made by the trustee, irrespective of whether the trustee has caused damage to the trust property. Similarly, unauthorised transfers may be rescinded, if a third-party knew or should have known the illegitimate

253Stylianou, T (2020), Data Guidance, " South Korea: National Assembly passes proposed amendments to strengthen data protection legislation". Available at <<https://www.dataguidance.com/opinion/south-korea-national-assembly-passes-proposed>>

254 Personal Information Protection Act, Act No.16930, Feb 4, 2020. Available at https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG

255Stangarone, T (2020), The Diplomat, "South Korea's Digital New Deal " Available at <<https://thediplomat.com/2020/06/south-koreas-digital-new-deal/>>

256Min-kyung, J (2020), The Korea Herald, "S. Korea to focus on digital infrastructure investment, 'Data Dam' project: minister" Available at<<http://www.koreaherald.com/view.php?ud=20200911000726>>

257 Act No. 900 of Korean Trust Act, 1961

https://elaw.klri.re.kr/eng_service/lawView.do?hseq=1051&lang=ENG

258 Trust Act 2011, See https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=43240&type=sogan&key=9

259 Article 2 of Trust Act 2011

260 Article 63 of the Trust Act 2011

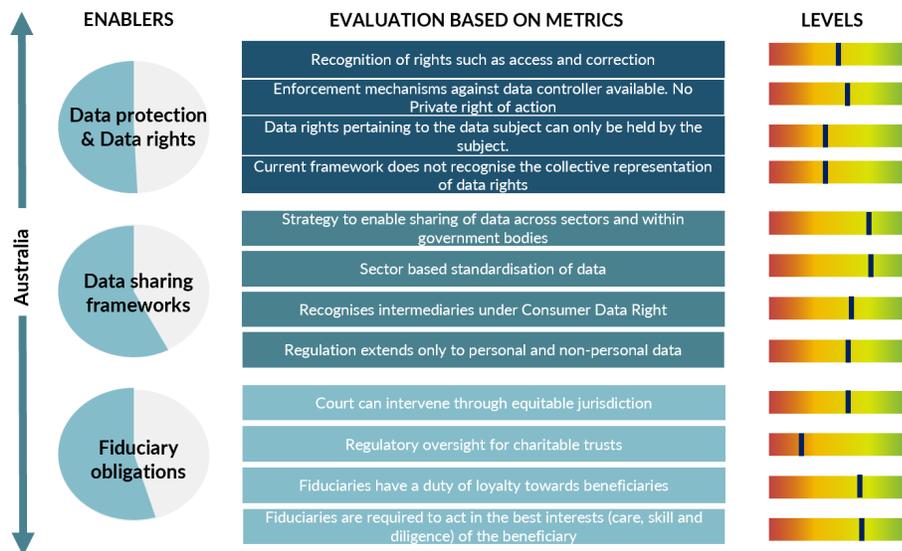
nature of the transfer.²⁶¹ Fiduciary relationships are also recognised in corporate structures, by which duties are imposed on directors/managers and investment business entities.

Key takeaways

South Korea is one of the few civil jurisdictions in South-east Asia that has codified trusts, and trustees' duties of care, loyalty, and impartiality. The PIPA is one of the few legislation that allows representatives to act on their behalf to exercise individuals rights over personal data. However, for the development of data trusts, data protection laws must bring about legal certainty on whether such rights to personal data can form the subject matter of these trusts.

While Korea has enacted comprehensive laws to regulate data use and sharing, it currently only recognises access, erasure, and correction rights. The proposed amendment to the PIPA is expected to define a new right to data portability. Along with the proposed PIPA amendment, there have also been advances in facilitating cross-sectoral sharing and policy-based approaches to data standardisation as part of the Digital New Deal. While initiatives such as MyData seek to increase the control which individuals have over their personal data, it remains to be seen how it incorporates procedural safeguards and accountability mechanisms.

7. Australia



Source
 Privacy Act
 OECD
 Data Availability and Transparency Bill
 Australian Charities and Not-for-profits Commission

a) Data Protection and Data Rights

Australia was one of the early countries that passed the Privacy Act 1988²⁶² to align with the OECD guidelines on the Protection of Privacy and Transborder Flows of Personal Data²⁶³. It gives individuals various rights such as the right to know why personal information is being collected and to whom it will be disclosed; the

261 Article 75(1) of the Trust Act 2011

262 Privacy Act 1988, see <https://www.legislation.gov.au/Series/C2004A03712>

263 OECD (2013), "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD." Available at: <https://www.oecd.org/sti/economy/oecdguidelinesonthe protection of privacy and transborder flows of personal data.htm>

right to access one's personal information; reject unwanted direct marketing, and the right to make a complaint.²⁶⁴ However, there is no private right of action against data controllers available to individuals.

The Australian Privacy Principles (APP) form the foundation of the privacy protection framework of the Act²⁶⁵. They apply to all entities the Act covers and governs the standards, rights and obligations around collection; use and disclosure of personal information; the entity's governance and accountability; integrity and correction of personal information and individual's rights to access their personal information²⁶⁶.

b) Data sharing frameworks

Following Europe and Canada, as a means to encourage data use for economic benefit, Australia released its first Data Strategy for 2021 to 2025²⁶⁷. The strategy seeks to strengthen effective, safe and secure data use. Amongst other functions, the strategy will also outline the government's frameworks surrounding data sharing and custodianship of both public and private data in Australia. Additionally, the government initiative plans to incorporate inter-agency (government) collaboration in order to promote data maturity, visibility and capability in the Australian Public Service²⁶⁸. As part of their data-driven innovation approach, the Data Strategy is set out to construct a framework to improve data sharing mechanisms, data access management and bolster participation between government and businesses. In order to achieve this, the government looks at the possibility of incorporating Consumer Data Right and relevant institutions to establish a data-driven economy²⁶⁹.

There are some intra-jurisdiction data sharing channels in place in Australian jurisdiction at varying levels such as the Multi-Agency Data Integration Project (MADIP) which integrates datasets from five jurisdictions - the Australian Bureau of Statistics; the Australian Taxation Office; Department of Education, Skill and Employment; Department of Health; Department of Social Services and Services Australia²⁷⁰.

Recently, the Australian government tabled Data Availability and Transparency Bill 2020²⁷¹ and, if passed, will allow greater sharing of public sector data with accredited users - either from public or private sectors for the purposes of improving government sector delivery, informing, and evaluating government policy and to support research and development. This will be permissible only if it is in accordance with the data sharing principles and governed by a data sharing agreement.²⁷²

c) Fiduciary Obligations

In Australia, duties owed by fiduciaries are determined as per the nature of the relationship.²⁷³ However, at the heart of these fiduciary relationships, the fiduciary undertakes to act on behalf of or in the interests of another person.²⁷⁴ Trusts in Australia largely follow principles of English trust law, with some variance codified through legislation. However, the fiduciary duty of loyalty and no-conflict are foundational to these relationships. In Australia, charitable trusts are regulated by the Australian Charities and Not-for-profits Commission.²⁷⁵ A charitable trust must be for a not-for-profit purpose that benefits the public.

Australia's data sharing frameworks take up a more comprehensive scope because of their robust inter-sectoral data sharing mechanisms and recognition of data intermediaries through the Consumer Data Right.

264See <<https://www.oaic.gov.au/privacy/the-privacy-act/rights-and-responsibilities/>>

265See<<https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles/>>

266 ibid.

267 Data and the Digital Economy, 2021. Available at <<https://digitaleconomy.pmc.gov.au/fact-sheets/data-and-digital-economy>>

268 ibid.

269 ibid.

270Australian Bureau of Statistics, Multi-Agency Data Integration Project (MADIP). Available at: <<https://www.abs.gov.au/about/data-services/data-integration/integrated-data/multi-agency-data-integration-project-madip>>

271Office of the National Data Commissioner,Data Availability and Transparency Bill,2020. Available at: <<https://www.datacommissioner.gov.au/data-legislation/data-availability-and-transparency-bill>>

272Office of the National Data Commissioner,Data Availability and Transparency Bill, 2020. Available at: <<https://www.datacommissioner.gov.au/data-legislation/data-availability-and-transparency-bill>>

273 Hospital Products Ltd v United States Corporation and Ors (1984)

274 ibid.

275 Australian Charities and Not-for-profits Commission, "Trusts", Available at: <<https://www.acnc.gov.au/for-charities/start-charity/before-you-start-charity/charity-subtypes/trusts-and-acnc>>

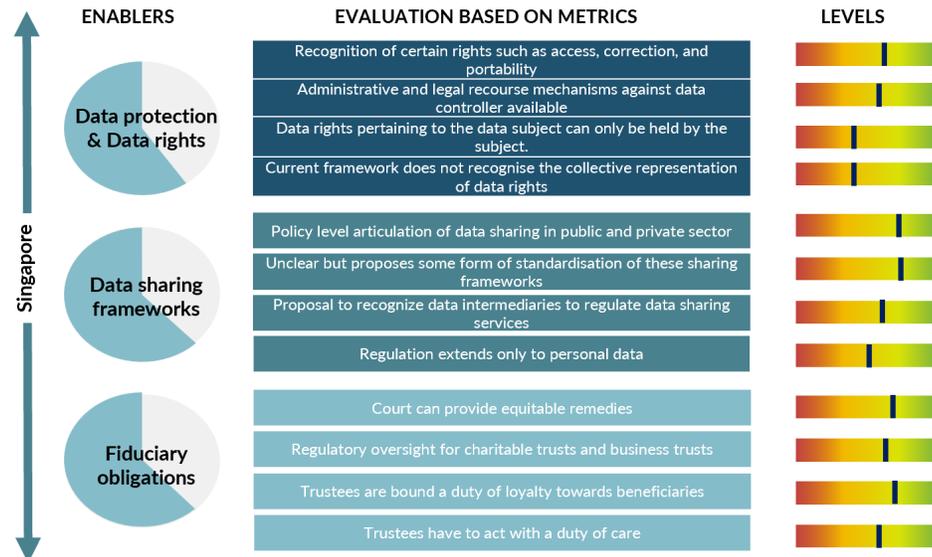
However, rights to portability and erasure are absent under the current data protection laws, creating barriers for individuals to withdraw their data from data holders. While Australia has delineated duties owed by trustees towards beneficiaries, fiduciary duties are prophylactic.

Key takeaways

While trusts in Australia primarily follow principles of English law, the absence of certain rights over personal data, such as portability and erasure of data, will restrict data trusts from managing the rights of the beneficiaries effectively. Alternatively, through the recent Consumer Data Right (CDR), the government is developing data sharing mechanisms that recognise a form of data portability right. CDR mandates entities in sectors to make consumer's data available to ease restrictions on accessing and sharing data. Consumers can then decide which providers they wish to share this data with. Currently, CDR has been implemented in the banking sector and is expected to roll out gradually across the various sectors.

Although current regulations under the CDR are silent on the representation of rights by third parties, there is potential to recognise data trusts as a new class of intermediaries that can manage the interests of the users while being bound by fiduciary obligations that are applicable to trustees.

8. Singapore



Sources:
 Personal Data Protection Act, 2013
 Digital Government Blueprint
 AI Singapore
 Trustees Act
 Business Trusts Act

a) Data protection and Data rights

The regulation of personal data and the rights conferred to individuals are defined in the Personal Data Protection Act (PDPA), which came into force in 2013.²⁷⁶ In addition to the PDPA, which is the overarching personal data protection law, there are other sector specific legislation like the Banking Act and the Insurance Act that regulate use of personal information.

Through flexible consent mechanisms, the PDPA seeks to balance the interests of individuals and the private sector.²⁷⁷ PDPA creates exemptions from requiring consent when processing "is necessary for any purpose

²⁷⁶ See <https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act>

²⁷⁷ *ibid.*

which is clearly in the interests of the individual or if the individual would not reasonably be expected to withhold consent." Additionally the PDPA confers rights to access, correction, and portability to individuals.²⁷⁸

b) Data sharing frameworks

Data sharing in Singapore is primarily driven by government efforts and investment in building digital capacity. For instance, the Digital Government Blueprint - five year plan put forward by Smart Nation and Digital Government Group - prioritises building open data platforms which use open application programming interfaces (APIs) and open standards for interoperability.²⁷⁹ Similarly, AI Singapore, a government wide partnership, brings together research institutions across the country to boost its AI capabilities. Additionally, the programme's Model AI Governance Framework provides guidance to the private sector organizations to address key ethical and governance issues for AI related solutions. The 'Implementation and Self-Assessment Guide' helps organisations assess the alignment of their AI governance practices to the framework.²⁸⁰

To boost sharing and re-use of data in the private sector, Infocomm Development Authority and the Personal Data Protection Commission (PDPC) introduced the Trusted Data Sharing Framework. It focuses on aspects that can guide commercial and non-governmental sectors to enhance data sharing within the ecosystem. The framework covers four aspects, namely, data-sharing strategy; legal and regulatory considerations; technical and organisation considerations; and operationalising data sharing.²⁸¹

Regulatory approaches to data protection have also attempted to encourage innovation in emerging technologies. This can be seen in the PDPC's flexibility to data protection, wherein it grants exemptions - on a case-by-case basis - to obligations under the PDPA for the development of new technologies.²⁸²

c) Fiduciary obligations

Singapore's legal system derives heavily from the English common law system, and therefore recognises common law conceptions of trusts and fiduciaries. While English law cases continue to hold relevance, their legal system has also codified some of the common law principles of trust and equity in the Trustees Act (Chapter 337)²⁸³ and the Business Trusts Act.²⁸⁴ Singapore views fiduciary duties as proscriptive and prophylactic, placing emphasis on the duty of loyalty and avoiding conflicts of interest.²⁸⁵ Under Singapore law, the main financial remedies available to the beneficiary are equitable compensation and account of profits²⁸⁶.

Unlike traditional trusts, business trusts import corporate governance-like mechanisms in the trust structure. A key difference is that the role of trustees is replaced by trustee-managers, which must be registered corporations.²⁸⁷ Although trustee-managers are not defined as fiduciary in nature, the duties are similar to ordinary trustees. So, while trustee-managers are required to act in the best interests of all the unitholders as a whole, they are required to prioritise the interests of the trusts over theirs only if it "conflicts with the interests of all the unitholders as a whole".²⁸⁸ Like most corporate regulations, the Business Trusts Act seeks to ensure accountability by imposing obligations on trustee-managers to conduct audits and hold annual general meetings. The registration and functioning of business trusts is also regulated by the Monetary Authority of Singapore.

278 *ibid*

279 GovTech Singapore, Digital Government Blueprint. Available at: <<https://www.tech.gov.sg/digital-government-blueprint/>>.

280 Infocomm Media Development Authority, Artificial Intelligence Available at: <<https://www.imda.gov.sg/AI-and-Data>>

281 Infocomm Media Development Authority (2021), "Trusted Data Sharing Framework." Available at: <<https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf>>

282 Infocomm Media Development Authority (2021), "Trusted Data Sharing Framework." Available at: <<https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf>>

283 See <https://sso.agc.gov.sg/Act/TA1967>

284 See <https://sso.agc.gov.sg/Act/BTA2004>

285 *Singapore Swimming Club v Koh Sin Chong Freddie* [2016] SGCA 28

286 YIP, Man and GOH, Yihan (2016) "Navigating the maze: Making sense of equitable compensation and account of profits for breach of fiduciary duty" Accessible at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2856131

287 Section 6 of the Business Trusts Act

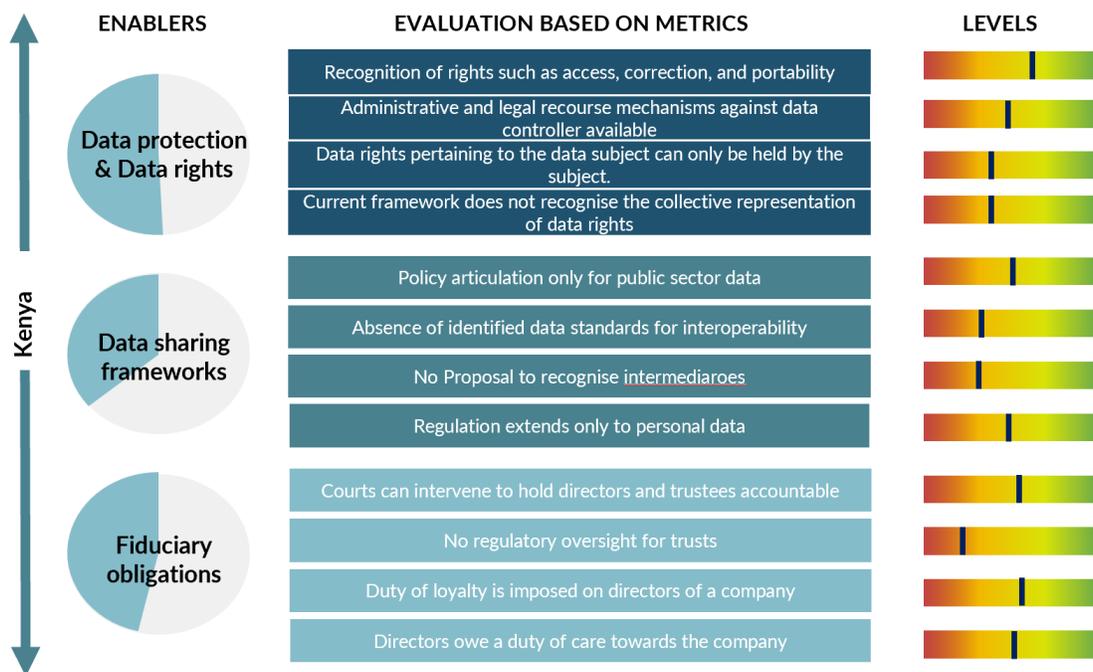
288 Section 10 of the Business Trusts Act

Key takeaways

Singapore's data-sharing frameworks are considerably more robust, with defined data-sharing mechanisms in the public and private sectors. In recent years, the discourse has also moved around data standardisation and recognition of data intermediaries, with the regulator encouraging data reuse for economic activity.

The flexibility of trusts in Singapore to engage in a wide range of activities and the recognition of rights over data such as access, portability, and erasure create a conducive ecosystem for the development of data trusts. The court's jurisdiction to oversee the actions of trustees provides beneficiaries with strong safeguards to ensure accountability.

9. Kenya



Sources:
 Kenya Open Data (ICT Authority)
 Data Protection Act, 2019
 Companies Act, 2015
 Trustees (Perpetual Succession) Act

a) Data protection and Data rights

Kenya's framing of data protection and the rights of data subjects are relatively latent. Regulation of information processing is primarily governed by the Data Protection Act 2019, which was enacted to recognise the right to privacy guaranteed under the recently redrafted Constitution of Kenya.²⁸⁹

Among other rights, the Data Protection Act confers data subjects with the rights to access, request information on their data processing, correction, and portability. The law also imposes restrictions on the flow of personal data outside its borders. Data can only be transferred across borders if there is adequate data protection safeguards or consent from the data subject.

b) Data Sharing

289 Article 31(c) and (d)

Owing to infrastructural barriers and legislative gaps, purpose or sector specific data sharing practices in Kenya are not prevalent. In the public sector, the Kenyan government In 2011, launched the Kenya Open Data Initiative (KODI), as part of its commitment - under the-then newly codified constitution - to provide citizens with access to information.²⁹⁰ Since its inception, KODI has made over 800+ datasets relating to government sectors such as health, education and infrastructure publicly available.²⁹¹

c) Fiduciary obligations

Given Kenya's common law origins, the legal system recognises the operation of trusts. The Trustees (Perpetual Succession Act specifies the rules regarding the incorporation of trusts for religious, educational, literary, scientific, social, athletic, or charitable purposes are defined in the Trustees (Perpetual Succession) Act.

Equally, fiduciary-like duties, such as exercising care and skill and avoiding conflicts of interest, are also recognised in agency relationships and corporate frameworks. (directors duties).²⁹² For instance, section 145 of the Companies Act 2015 codifies the duty of care, skill, and diligence owed by a director. Similarly, section 146 of the Act requires directors to avoid situations that can lead to conflicts of interest. However, directors owe these duties to the company and not the shareholders. Courts can intervene to remove/appoint new trustees or hold directors liable for breach of fiduciary duty.

Key takeaways

Although Kenya's recently enacted data protection law recognises individuals' rights to access, correct, and port their data, weak digital infrastructures and regulatory capacity have stultified discourse at an ecosystem level on the potential to steward data. Naturally, restrictions on access and availability of data have a bearing on data trusts and other data stewardship models to represent the interests of beneficiaries. In recent times, civil society organisations, such as the Open Institute, have been focusing their efforts on creating awareness and building networks to communicate the data rights afforded to individuals.

In addition to the considerations on the representation of data rights within trust structures, it is equally important to investigate the general acceptance of trusts within the jurisdiction's legal culture. Like South Africa, Kenya has a perceptible reliance on corporate frameworks like companies and agencies and is reflected in the manner in which company law has evolved in Kenya.

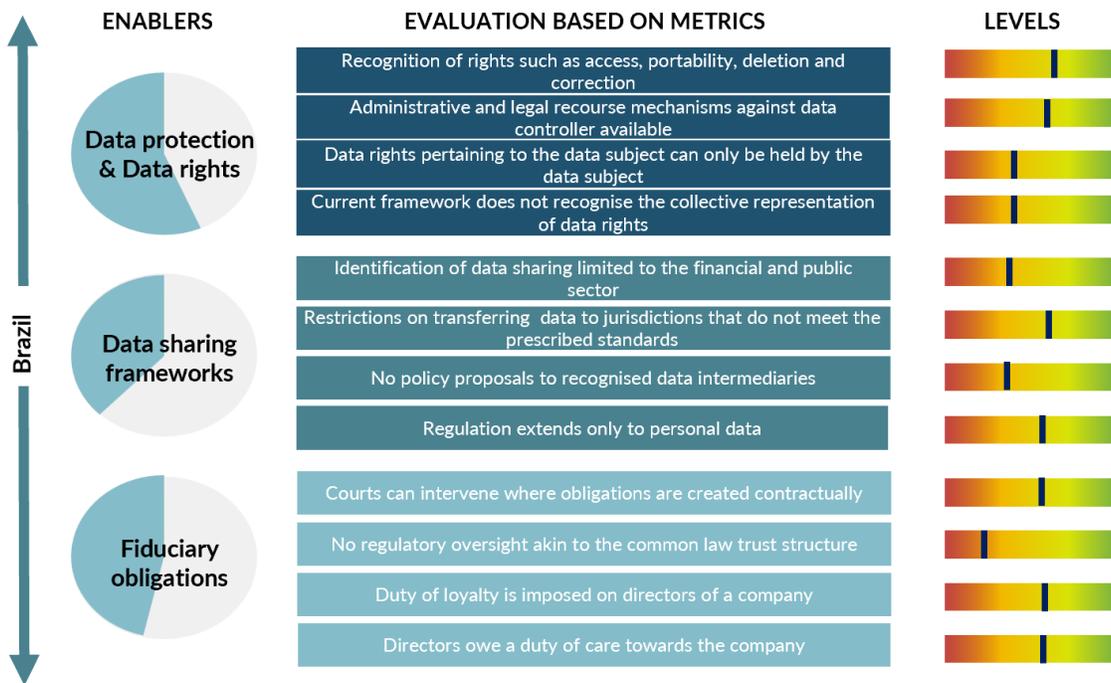
290 See <https://www.centreforpublicimpact.org/case-study/open-data-kenya>

291 See <https://www.opendata.go.ke/>

292 Sections 145 and 146 of the Companies Act 2015 Available at

http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2015/TheCompaniesAct_No17of2015_RevisedCompressed.pdf

10. Brazil



Sources:
 Brazil Corporations Act 1976
 Brazilian Civil Code
 LGPD Law No. 13.709

a) Data protection and Data rights

Although Brazil has various sectoral privacy laws in place, the enactment of the General Personal Data Protection Law (LGPD) was Brazil's first attempt at a comprehensive GDPR-like regulation of personal data. The LGPD derives heavily from the principles defined in the GDPR, especially with regard to the scope, territorial application and obligations under the law. Like with GDPR, anonymised data falls outside the ambit of regulation.

The legislation grants rights such as access to data, rectification, portability, opposition to treatment, right to information and explanation about the use of data. Interestingly, Article 40 of the LGPD gives the national data protection authority powers to prescribe standards for interoperability for portability. This may allow

b) Data Sharing

Brazil was one of the founding members of the Open Government Partnership 2011, which sought to promote transparency and availability of resources through the use of Information and Communication Technology.²⁹³ The technical standards and standardisation of formats are overseen by the National Open Data Infrastructure.²⁹⁴ However, purpose led data sharing in Brazil is still latent, with limited policy articulation of interoperability standards.

293 C. Bittencourt, J. Estima and G. Pestana (2019), 14th Iberian Conference on Information Systems and Technologies (CISTI), "Open Data Initiatives in Brazil", doi: 10.23919/CISTI.2019.8760592

294 See <https://cnae.ibge.gov.br/en/estrutura/natjur-estrutura/natureza-juridica-2003-1/1861-novo-portal/institucional/8814-infraestrutura-nacional-de-dados-abertos-inda-2.html>

In the financial sector, the Brazilian Central Bank is in the process of increasing the flow of data in the banking sector through application programming interfaces (APIs) that will give third-party developers access to consumer transaction data to build applications and services around the participating financial institutions.²⁹⁵

c) Fiduciary obligations

As a civil legal system, Brazilian law does not recognise trusts. While the conception of fiduciary law is largely absent, duties like care and diligence are imposed on directors - which they owe towards the company - through the Brazilian Corporation Law.²⁹⁶ There are other legal entities like foundations and associations that allow the collective administration of assets for charitable purposes. Associations can be formed by two or more persons for non-profit purposes. An association's Articles of Organization describe its purpose, rules around the admission and dismissal of the association members, and manner in which board/management functions.

While associations can be constituted for any purpose, foundations are required to have a public interest element. Like charities, foundations could be public or private, and are created for specific purposes of public interest by way of an endowment.²⁹⁷ The Brazilian Civil Code lists different areas for which they can be established. For private foundations, accountability is maintained through oversight powers of the Attorney General's Office.²⁹⁸ Public foundations are created by the government through legislation to undertake activities that do not ordinarily fall within the government's remit. However, in both these structures, it is unclear how data (or the rights over it) could be managed and if fiduciary-like obligations exist within it. Both foundations and associations require members to forgo proprietary interests over the assets (data/data rights in the case of data trusts).

Key takeaways

Brazil's enactment of the LGPD in 2018 culminated in a decade-long movement involving participation from academia, civil society, and the private sector.²⁹⁹ Like GDPR, the Brazilian law recognises rights such as access, portability, and deletion, which are necessary for data intermediaries to manage the interests of individuals.

However, like most jurisdictions that have recently enacted a data protection law, the limited discourse at a grassroots level on the rights available to individuals over their personal data has meant that regulators' efforts have been concentrated on creating awareness and ensuring compliance with the law.³⁰⁰ For instance, in a survey conducted in September 2020 by a Brazilian credit intelligence company, 70% of respondents were unaware of the LGPD.³⁰¹

Developing a data governance approach that relies on the trust framework in the absence of common law trust-like structures will prove challenging. Conceptualising data trusts require legislative intervention that allows for collectivised representation and management of rights over data with avenues to hold trustees or managers accountable.

295 Mari,A (2019) "Brazil ushers in open banking model" Available at <https://www.zdnet.com/article/brazil-ushers-in-open-banking-model/>

296 Article 153 of the Brazilian Corporation law http://conteudo.cvm.gov.br/export/sites/cvm/subportal_inlgles/menu/investors/anexos/Law-6.404-ing.pdf

297 See http://www.planalto.gov.br/ccivil_03/leis/l7596.htm

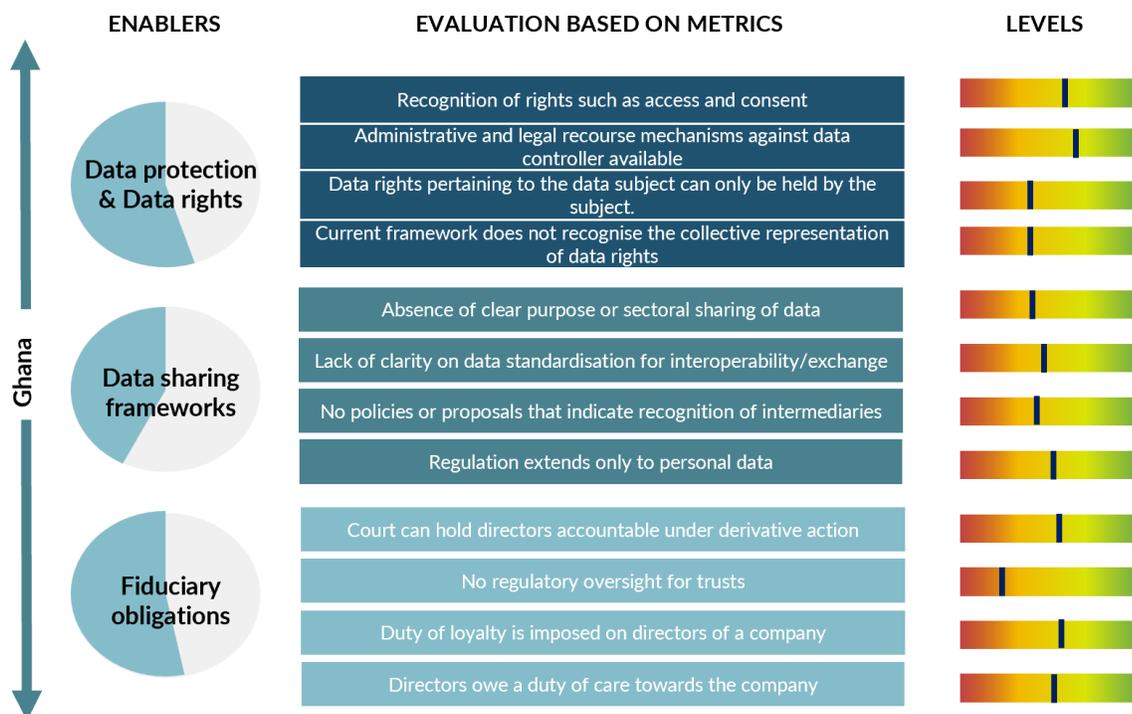
298 Civil Code Article 66

299 See <https://www.observatoriodoprivacidade.com.br/en/memorial/2018-an-astral-conjunction-2/>

300 Mari,A (2021) "Brazilian government launches data protection campaign" Available at <https://www.zdnet.com/article/brazilian-government-launches-data-protection-campaign/>

301 Mari, A (2020) "Brazilians mostly unaware of data protection regulations" Available at <https://www.zdnet.com/article/brazilians-mostly-unaware-of-data-protection-regulations/>

11. Ghana



Sources:
Corporations Act, 2019
Data Protection Act, 2012

a) Data Protection and Data Rights

In Ghana, data protection is primarily governed through the Data Protection Act, 2012.³⁰² In addition to this, there are other laws such as the Electronic Communications Act, 2008, Electronic Communications Regulations, 2011 and the Credit Reporting Act, 2007 which have provisions on the use of data. In comparison to other countries, Ghana's Data Protection Act is comparatively narrow in its scope. Data subjects have the right to access and correct their personal data, and object to processing of their personal data. While there are no data localisation laws in place, Ghana's data protection laws mandate data controllers and processors in Ghana to apply foreign countries' data protection laws when processing foreign citizens' personal data.

b) Data sharing frameworks

While Ghana sees an absence of policy and legislative articulation on data sharing, there are some instances of public-private sector collaboration for data sharing. For instance, in 2018, Ghana Statistical Service (GSS), Vodafone Ghana, and Flowminder signed a data sharing agreement to formulate public health and sustainable development policies by drawing insights from mobile phone data.³⁰³ Pseudonymised and aggregated data was shared with GSS with limitations on use. The collaboration has continued during the pandemic to assess the effectiveness of COVID-19 restrictions by providing insights upon internal migration, aggregated mobility patterns and reductions in movement during the pandemic³⁰⁴. With the public sector facing constraints in the availability of good datasets, such collaborations with private technology corporations allow decision makers access to data that can be leveraged to create targeted policies.

³⁰² See https://cybersecurity.gov.gh/documents/Data_Protection_Act_2012.pdf

³⁰³ See <https://www.unsdsn.org/post-title61e7c848>

³⁰⁴ See https://static1.squarespace.com/static/5b4f63e14eddec374f416232/t/5ef206529723f531491dceb0/1592919639048/Ghana+Case+Study_FINAL.pdf

c) Fiduciary obligations

In Ghana, fiduciary obligations and relationships are most clearly located in duties owed by directors of companies. The recently enacted Companies Act, 2019 holds that directors stand in a fiduciary relationship towards the company. Directors must act in the best interests of the company, and promote the purposes of the company with good faith, diligence and care.³⁰⁵

Such a model for data trusts would require creating a corporate structure where the company has contractual arrangements with each data provider, who act in their capacity as shareholders of the company. The data transferred to the company would be managed by the directors bound by duties recognised in the Companies Act.³⁰⁶ Under the Companies Act, shareholders have the power to bring derivative action against the director for any breach of breach of fiduciary responsibilities.³⁰⁷

Key takeaways

The recognition of rights in Ghana's data protection law and the established administrative and legal recourse mechanisms against data controllers make the country's data protection and data rights ambit more optimistic. Further, interactions with experts reflected a strong political will to realise the value of data, as well as a great degree of cooperation between policymakers, regulators and the private sector. However, lack of lucid data standardisation policies, combined with a dearth of sectoral data sharing without clear purpose do not fare well for Ghana's data sharing frameworks. In building Ghanaian data regimes, a lack of capital has also hampered on-ground advocacy and implementation of such rights. The adoption and reliance on trusts to administer assets are unclear. On the contrary, the Companies Act imposes fiduciary duties on the directors of the company. However, these duties are owed towards the company and not the shareholders.

305 Section 190 of the Companies Act, 2019, Available at <https://rgd.gov.gh/docs/Act%20992.pdf>

306 See <https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf>

307 Section 201 of the Companies Act, 2019

SECTION 4

The final section presents the takeaways and insights from our comparative analysis of the jurisdictions, identifying the various challenges and uncertainties in the current ecosystem to develop data trusts. The latter part of the section also outlines areas that are not within the report's scope but merit further research and exploration. Important takeaways and insights from the section include:

- The articulation of data rights and data sharing frameworks varied significantly across different jurisdictions. This was due to a range of factors such as economic and political constraints, lack of political will, and disparity in digital infrastructures.
- While certain jurisdictions like the EU, UK, and Brazil had robust recognition of personal data rights, many of them lacked the range of rights - such as access, portability, and erasure - required for the operation of data trusts. Even in jurisdictions that did recognise them, there were limitations to its exercise.
- Through expert interviews, it was observed that even in jurisdictions where there was legislative recognition of rights and concepts, the ground reality was quite different. So, while certain jurisdictions recognise trusts and have enacted comprehensive data protection laws, the actual adoption and implementation might vary significantly.

4.1 Insights and recommendations from comparative analysis

#	Region	Legal Enablers			Highlights
		Data rights & Protection	Data Sharing	Fiduciary Obligations	
1	Germany				Proposals to recognise intermediaries alongside European data spaces and market.
2	England & Wales				Presence of data rights and legal structure necessary for data trusts.
3	India				Proposes 'consent managers' as platforms that can mediate individual's consent.
4	Canada				Has both civil and common law trusts. Quebec civil trusts do not require transfer of ownership
5	South Africa				Recognises trusts that allow beneficiaries to have ownership over trust property
6	South Korea				Civil legal system with codified trusts. Allows exercise of data rights by representatives.
7	Australia				Policy move across sectors to mandate entities to make data available to consumers
8	Singapore				Codified 'business trusts' that have proactive corporate like mechanisms for accountability
9	Kenya				Recently enacted a comprehensive personal data protection law. Limited data sharing frameworks
10	Brazil				Recently enacted a comprehensive personal data protection law. Does not recognize trusts.
11	Ghana				Regulatory role still nascent but move towards public-private partnerships for data sharing.

Our analysis throws up several key insights that demonstrate disparity in maturity of legal landscapes for data trusts around the globe, and point to the need for administrative and legislative investments in data

governance in several countries. Further, it was found that for legal systems which don't embed fiduciary duties matching common law structures, there may be a need to explore diverse structures of human-centric data governance.

Disparity across nations and the lack of digital infrastructure

Given the diversity - both economic and political - of the jurisdictions analysed we found that the maturity in articulating rights over data varied significantly. This was partly due to varied priorities for different jurisdictions, economic and political constraints, or the lack of political will to articulate these rights. When evaluating data-sharing policies, it is clear that the robustness of digital and technical pathways infrastructures plays a vital part. This includes regulatory measures like standardisation of data formats or sharing purpose, enabling interoperability, or introducing digital public infrastructure. For developing countries, the absence of data sharing policies is often a function of digitisation capacity. Many countries rely on international technology companies to set up this infrastructure, which often comes with restrictions on how governments can share or use this generated data.

Thus, the legal analysis must be read in cognisance of the fact that developed countries such as those in the European Union have, over the years, been able to take advantage of their economic wealth and social awareness to prioritise sturdy digital infrastructures. Therefore, the discourse and ecosystem around regulation of technologies, data protection and data rights is much more robust and it is unsurprising that a progressive and foundational regulation such as the GDPR has emerged out of the EU. Similarly, countries such as Australia, Canada, Singapore are also making advances on data protection.

In most of the developing world, digital ecosystems are defined by infrastructure created by western technology corporations. While this influence has enabled these jurisdictions to streamline governance and improve access to digitised financial services, they are prevented from deriving full value from the data generated. Countries like Kenya, India, and South Africa have started responding to some of these concerns by framing data localisation laws and policies, applying the lens of 'data sovereignty'. However, this demands durable, low-friction digital infrastructure that can responsibly collect and process large amounts of data. Given these tensions, it is often quite difficult for governments to strike a balance between regulation, protectionism and liberalization.

Personal data rights and building for autonomy

Even within some of the countries with more robust digital infrastructures, the absence of certain personal data rights - such as access, portability and erasure - pose challenges in creating a sustainable data trust ecosystem. For instance, Canada, Australia, and South Korea, while faring well on digital infrastructure, have yet to recognise clear data portability rights. It was found that in order to enable data trusts in a streamlined ecosystem - infrastructure alone cannot carry the torch, and personal data rights must mature to enable greater individual autonomy. This also entails exploration of novel ways in which individuals can exercise their rights over data which, in turn, may allow means for collective governance (for example, with the ability to pool data).

On the other hand, while some developing countries fared better in recognising these rights, through conversations with multiple experts (which have helped contextualise this work) it was found that there is often a dissonance between the provisions of legislation and its actual enforcement. For instance, in a November 2020 survey conducted by the Brazilian Association of Software Companies (ABES) and EY, it was observed that nearly 60% of the corporations in the technology sector were yet to comply with the provisions of the LGPD. Thus, for most of these nations, there is a need to not only enable a fertile legal landscape for data trusts, but to build capacity, awareness and process-oriented enforcement.

In order to map individual data rights to the trust structure, a certain level of mandatability or transference of rights is necessitated. In order for a trustee to manage a subject's data, there must be clear legal outlines as to what level of an individual's autonomy over their data can come within the ambit of third party delegation. Consequently, the aim of fiduciary relationships is partly to protect beneficiaries and guard against the resultant power dynamic between beneficiary and trustee. However, such a transference - which enables trustees to exercise data rights on behalf of the beneficiary - is an incredibly delicate and contentious legal space, and there is a need to guard against paternalistic structures that delegation of data rights may enable.

Legislative implementation and regulatory oversight

The marked variance in legislative process and the implementation of laws has been a recurring feature in this analysis. Legal concepts that are common across jurisdictions are not always implemented uniformly. For instance, the extent of adoption of trusts in Kenya and South Africa - countries with common law origins - is not as crystallised as compared to jurisdictions such as England, which extensively use trusts for a variety of commercial and non-commercial purposes. Therefore, the feasibility of trusts remains an underdeveloped and underexplored area of law.

Although charitable trusts in the UK and Australia, and business trusts in Singapore have established regulatory regimes, a common thread across most jurisdictions was the absence of institutionalised oversight mechanisms that can regulate data trusts. Regulatory authorities can incorporate flexible methods to navigate challenges while giving legitimacy and certainty to the activities of data trusts. Ex-ante and ex-post regulatory powers also ensure accountability and are invaluable in jurisdictions where court processes are costly. Unlike legislative approaches, which are typically binding and slow to change, regulators can adopt more participatory practices that reflect the concerns of stakeholders from the private sector, academia, and civil society.

The success of the regulator will depend on how it contextualises its approach. Considering the nascent stage at which data trusts are in practice, regulators must play a much more proactive and reflexive role in creating awareness, engaging different stakeholders in the ecosystem, and guarding against regulatory and ecosystem capture. However, any such approach will require investments in building regulatory capacity.

A 'data trust conundrum' for stewardship

It is evident that the conception of data trusts is most fundamentally rooted in English trust law. Based on this analysis, even in jurisdictions that have common law influence and recognise trusts, the evolution of its concepts have not mirrored the English experience. This is even more the case when considering gaps and uncertainties around the ability for data rights to form the subject matter of trusts. In some of the commonwealth jurisdictions, the codification of trusts may have restricted its scope.³⁰⁸

The case studies chronicled in Output 1 (Data Trust Survey) showcase a diversity of initiatives that empower communities and individuals to steward data. These case studies highlight the bottom-up approach and show differences in structures such as MIDATA and Driver's Seat are data co-operatives; they focus on community empowerment and managing data use with data generators participation. Further, Output 1 also presents a result of a survey targeting practitioners who are building trusts and how these initiatives have identified themselves and their approach. The survey lays down 6 functions of data trusts as per GPAI definition. Respondents who performed all 6 functions were either not active or preferred not to be called data trusts. Legal barriers such as clarity on data rights of citizens, variation of data rights across different jurisdictions or even having an operative data protection legislation in the first place, and the ambiguity in recognition of trusts and whether trusts can hold data (or rights over it) could be the reason why initiatives fail to meet the conception of data trusts.

Given this, our analysis has attempted to locate functionally equivalent provisions in these jurisdictions. By identifying, for instance, fiduciary-like duties and the scope for similar judicial interventions that are contained in trust structures. Yet this application has not been a straightforward exercise. For instance, while civil legal systems such as Germany recognise higher standards of care and good faith in contractual obligations when compared with common law systems, it is still not feasible to draw parallels with the fiduciary relationship between a trustee and beneficiary where the scope of remedies available are very different. These complexities have raised a keen awareness that the trust structure may not be one that can be resurrected in a uniform manner across most legal systems.

However, as we work toward the goal of enabling value oriented, human-centric data governance, there is promise in a number of jurisdictions (based on their performance across the key legal enablers) to develop trust-like structures and alternate models of data stewardship. In regions like Singapore, Canada, South Korea or Germany, for example, there is favourable alignment across the analysis framework and while it may be arduous to build data trusts in particular, there is certainly potential to broaden the horizon of

³⁰⁸ Refer to box 'Can data rights form the subject matter of trusts across jurisdictions'

stewardship to models like data cooperatives, data exchanges, collaboratives or others. It is important to guard against a pigeonhole of stewardship that foregrounds data trusts even in regions where other modes of governance can minimise legislative overhaul and friction, while still working to maximise participation, agency and value.

Thus, it is critical to note that the analysis reflects legal fertility for only data trusts as defined in aforementioned sections³⁰⁹, and the outcomes or levels depicted must not be confused to be a decree on the overall robustness of a region's data regime. Many of the jurisdictions captured are better suited to other models of data stewardship, and there is a need to amplify discourse, tests and enable human centric data governance in ways that play to the strengths of various legal systems. And for many, these strengths are not most ideally captured by trust law.

4.2 Scope of the research - open questions

While this analysis has encompassed the legal necessities, status and challenges in implementing data trusts, there are a number of limitations that feature beyond the scope of this review, and are yet pertinent in the exploration of data trusts and other human centric forms of data governance.

While the framing of personal data rights has individuals at its focal point, an area that merits exploration is the consequence of collectivising these rights under trusts. A critical question that needs to be addressed is how regulations propose to balance collective interests and individuals' interests. Equally, what avenues for recourse will aggrieved minority groups in a data trust have, and how can personal data rights be disaggregated from the collectivised rights and interests?

Intellectual property rights (IPR) claims over data held by organisations can also create barriers to the portability of data to data trusts, specifically in the case of inferred data, which is not provided by the data generator. While the tensions between IPR and data protection laws currently curtail individuals' right to port inferred data, the possibility of collective data rights - as articulated in India for non-personal data - over aggregated data and the role of data trusts to negotiate these tensions needs to be evaluated.

Discussions in Europe - under the proposed Data Act - and the U.S. on the framing of co-generated rights also pose new questions on the possibility of data trusts to hold co-generated data.³¹⁰ The feasibility for data trusts to hold these data rights will depend on how co-generated rights are framed, and extent to which data generators are granted rights over, for instance, the portability rights afforded to them.

At a foundational level, trusts offer an institutional framework for data trusts to operate. The nature of a trust's functions will depend on its governance structure and the interests that individual data trusts wish to achieve. Building a plurality of data trusts that pursue diverse interests, among other factors, depends on the articulation of revenue models. It is vital to explore incentivisation structures that can foster trustees to pursue their beneficiaries' interests proactively.

309 Data Governance Working Group (2021), Global Partnership for Artificial Intelligence, "Understanding data trusts", <https://ceimia.org/wp-content/uploads/2021/07/2021-07-09-GPAI-summary-understanding-data-trusts-updated.docx.pdf>

310 See <https://www.europeanlawinstitute.eu/projects-publications/completed-projects-old/data-economy/>

SECTION 5

5.1 About Aapti Institute, and GPAI

Aapti Institute is a public research firm that works at the intersection of technology and society, building policy-relevant and actionable insights on the digital economy. It was founded in 2019 in Bangalore, India. Through its Data Economy Lab, a flagship effort to rebalance power in the digital economy, Aapti supports research, conversation and experimentation around the practice of data stewardship.

The **Global Partnership on Artificial Intelligence (GPAI)** is a multi-stakeholder initiative which aims to bridge the gap between theory and practice on AI by supporting cutting-edge research and applied activities on AI-related priorities. Built around a shared commitment to the OECD Recommendation on Artificial Intelligence, GPAI brings together engaged minds and expertise from science, industry, civil society, governments, international organisations and academia to foster international cooperation.

5.2 Authors

This report was written by Amrita Nanda, Bilal Mohamed and Astha Kapoor from Aapti Institute. The report was written in collaboration with the GPAI Data Working Group, whose insight and expertise helped to shape the direction, content and focus of this report.

5.3 Report drafting

This report was written in the autumn of 2021, with the research taking place over the summer. The literature review, expert interviews and analysis took place over July and August which was followed by drafting of the report in September. The first draft of the report was reviewed by GPAI in late September.

5.4 Acknowledgements

We would like to thank GPAI for giving us the opportunity and funding to conduct this research and write this report, and for supporting the research with their knowledge and passion. We also thank the experts who made time for interviews - their insights form the basis of this report.

SECTION 6

Complete bibliography

Primary Literature (Legislation and Policies)

Legislation/Policy/ Govt. portals	Country	Link
Brazilian Corporation Law	Brazil	http://conteudo.cvm.gov.br/export/sites/cvm/subportal_ingles/menu/investors/anexos/Law-6.404-ing.pdf
Data Protection Act 2012	Ghana	https://cybersecurity.gov.gh/documents/Data Protection Act 2012.pdf
Companies Act 2015	Kenya	http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2015/TheCompaniesAct_No17of2015_RevisedCompressed.pdf
Open Data Kenya	Kenya	https://www.opendata.go.ke/
Companies Act 2019	Ghana	https://rgd.gov.gh/docs/Act%201992.pdf
Trusted Data Sharing Framework.	Singapore	https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf
Artificial Intelligence - Infocomm Media Development Authority.	Singapore	https://www.imda.gov.sg/AI-and-Data

Digital Government Blueprint	Singapore	< https://www.tech.gov.sg/digital-government-blueprint/ >.
The Personal Data Protection Act (PDPA)	Singapore	https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act >
Australian Charities and Not-for-profits Commission. <i>Trusts</i> .	Australia	< https://www.acnc.gov.au/for-charities/start-charity/before-you-start-charity/charity-subtypes/trusts-and-acnc >
Data Availability and Transparency Bill ,ONDC, 2020	Australia	< https://www.datacommissioner.gov.au/data-legislation/data-availability-and-transparency-bill >
Australian Bureau of Statistics. Multi-Agency Data Integration Project (MADIP).	Australia	< https://www.abs.gov.au/about/data-services/data-integration/integrated-data/multi-agency-data-integration-project-madip >
Data and the Digital Economy 2021	Australia	< https://digitaleconomy.pmc.gov.au/fact-sheets/data-and-digital-economy >
Australian Privacy Principles,OAIC,2014.	Australia	< https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles/ >
Privacy Act 1988	Australia	https://www.legislation.gov.au/Details/C2021C00139
Korean Trust Act 1961	Korea	https://elaw.klri.re.kr/eng_service/lawView.do?hseq=1051&lang=ENG
Personal Information Protection Act 2011	Korea	https://www.privacy.go.kr/eng/about_us.do
Trust Property Control Act, 1988	South Africa	https://www.justice.gov.za/legislation/acts/1988-57.pdf
National Digital Health Strategy of South Africa	South Africa	https://www.health.gov.za/wp-content/uploads/2020/11/national-

		digital-strategy-for-south-africa-2019-2024-b.pdf
National Data and Cloud Policy	South Africa	https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf
Protection of Personal Information Act (POPIA) 2013	South Africa	https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf
Civil Code of Quebec	Canada	http://legisquebec.gouv.qc.ca/en/showdoc/cs/ccq-1991#:~:text=The%20Civil%20Code%20of%20Qu%C3%A9bec,relations%20between%20persons%2C%20and%20property.&text=Every%20human%20being%20possesses%20juridical,full%20enjoyment%20of%20civil%20rights.
Canadian Data Governance Standardization Collaborative	Canada	https://www.scc.ca/en/flagships/data-governance
Pan-Canadian Health Data Strategy	Canada	https://www.canada.ca/en/public-health/programs/pan-canadian-health-data-strategy.html
Consumer Privacy Protection Act (CPPA) 2020	Canada	https://oag.ca.gov/privacy/ccpa
Digital Charter Implementation Act	Canada	https://www.ic.gc.ca/eic/site/062.nsf/eng/00120.html
Digital Privacy Act 2015	Canada	https://laws-lois.justice.gc.ca/eng/annualstatutes/2015_32/page-1.html
Personal Information Protection and Electronic Documents Act 2000	Canada	https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

National Digital Health Mission	India	https://ndhm.gov.in/
Trust Act 1882	India	https://legislative.gov.in/sites/default/files/A1882-02.pdf
Data Empowerment and Protection Architecture 2020	India	https://www.niti.gov.in/sites/default/files/2020-09/DEPA-Book.pdf
The Judicature Acts of 1873 and 1875	United Kingdom	https://www.parliament.uk/about/living-heritage/transformingsociety/laworder/court/overview/judicatureacts/
Data Sharing and Release Bill - New Australian Government Data Sharing and Release Legislation: Issues paper for consultation (2018)	Australia	https://pmc.gov.au/resource-centre/publicdata/issues-paper-data-sharing-releaselegislatio
Report by the Committee of Experts on Non-Personal Data Governance Framework (December 2020)	India	https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf
National Data Strategy	United Kingdom	https://www.gov.uk/guidance/national-data-strategy#:~:text=The%20National%20Data%20Strategy%20(NDS,p%20public%20trust%20in%20data%20use.
The Personal Data Protection Bill , 2019	India	http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf
Information Technology Act 2000	India	https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf
National Research Data Infrastructure , The German Research	Germany	< https://www.dfg.de/en/research_funding/programmes/nfdi/index.html >

Foundation (2021)		
What is Gaia-X?, Data Infrastructure EU (2020)	Germany	https://www.data-infrastructure.eu/GAIA/Navigation/EN/Home/home.html
White & Case (2020), German Bundestag passes second act on the adaptation of data protection law to the GDPR Second Data Protection Adaptation and Implementation Act EU	Germany	https://www.whitecase.com/publications/alert/german-bundestag-passes-second-act-adaptation-data-protection-law-gdpr
Federal Data Protection Act (BDSG) of 30 June 2017.	Germany	< https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html >
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act), 2020.	EU	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en
REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018: On a framework for the free flow of non personal data in the European Union.	EU	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN
Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act), 2020.	EU	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0767
A European strategy for data (2020), European Commission.	EU	https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-

		fit-digital-age/ european-data-strategy#document
General Data Protection Act	United Kingdom	https://www.gov.uk/data-protection#:~:text=The%20Data%20Protection%20Act%202018,Data%20Protection%20Regulation%20(GDPR).&text=They%20must%20make%20sure%20the,used%20fairly%2C%20lawfully%20and%20transparently
Business Trusts Act	Singapore	https://sso.agc.gov.sg/Act/BTA2004
General Data Protection Regulation (GDPR), 2018	EU	https://gdpr-info.eu/

Cases

1. *RBI vs Jayantilal Mistry*, TRANSFERRED CASE (CIVIL) NO. 91 OF 2015.
2. *Braun and Another v Botha and Another* (263/82) [1984] ZASCA 19
3. *Phillips v Fieldstone Africa (Pty)* 2004 (3) SA 465 (SCA)
4. *Hospital Products Ltd v United States Corporation and Ors* (1984)
5. *Singapore Swimming Club v Koh Sin Chong Freddie* [2016] SGCA 28

Secondary Literature

1. Ada Lovelace joint publication with AI Council. "Exploring legal mechanisms for data stewardship" (2021), Accessible at <https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/>
2. Balkin, Jack M., "Information Fiduciaries and the First Amendment." *U.C. Davis law review* 49.4 1183, 2016.
3. Blankertz, Aline and Specht, Louisa. "What regulation for data trusts should look like", 2021., Accessible at https://www.stiftung-nv.de/sites/default/files/regulation_for_data_trusts_0.pdf
4. Blankertz, Aline. "Designing Data Trusts", 2020. Accessible at https://www.stiftung-nv.de/sites/default/files/designing_data_trusts_e.pdf
5. BPE Solicitors, Pinsent Masons, and Chris Reed. " (2019) Data Trusts: Legal and Governance Considerations", Accessible at <https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf>
6. Buckle, Paul. "Data Trusts In Guernsey", 2021. Accessible at <https://www.ifcreview.com/articles/2021/march/data-trusts-in-guernsey/>
7. C. Bittencourt, J. Estima and G. Pestana, "Open Data Initiatives in Brazil," 14th Iberian Conference on Information Systems and Technologies (CISTI), 2019, pp. 1-4, doi: 10.23919/CISTI.2019.8760592
8. Clarry, Daniel. "FIDUCIARY OWNERSHIP AND TRUSTS IN A COMPARATIVE PERSPECTIVE." *The International and Comparative Law Quarterly*, vol. 63, no. 4, Cambridge University Press, 2014, pp. 901–33, Accessible at doi:10.1017/S0020589314000463.
9. Criddle, Evan J., et al. "The Oxford Handbook of Fiduciary Law", Edited by Evan J. Criddle, Paul B. Miller, and Robert H. Sitkoff, Oxford University Press, 2019
10. Data Privacy Brazil, Observatorio Privacy, accessible at <https://www.observatorioprivacidade.com.br/en/memoria/2018-an-astral-conjunction-2/>
11. "Data Trusts A new tool for data governance" , 2019 Retrieved from https://hello.elementai.com/rs/024-OAQ-547/images/Data_Trusts_EN_201914.pdf
12. Delacroix, Sylvie, and Neil D. Lawrence. "Bottom-up Data Trusts: Disturbing the "One Size Fits All" Approach to Data Governance". *International Data Privacy Law*, vol. 9, no., 2019, pp. 236–52, Accessible at <https://doi.org/10.1093/idpl/iphz014>.
13. Du Toit, F. "Jurisprudential milestones in the development of trust law in South Africa's mixed legal system", In L. Smith (Ed.), *The Worlds of the Trust* (pp. 257-276). Cambridge: Cambridge University Press, 2013. doi:10.1017/CBO9781139505994.012
14. Ducuing, Charlotte (2020). "Data rights in co-generated data': The ground-breaking proposal under development at ELI and ALI ",. accessible at <https://www.law.kuleuven.be/citip/blog/data-rights-in-co-generated-data-part-1/>
15. Gelter, Martin and Helleringer, Genevieve. "Fiduciary Principles in European Civil Law Systems", 2018. Available at <https://ssrn.com/abstract=3142202>
16. Gold, Andrew S., and Miller, Paul B. "Philosophical Foundations of Fiduciary Law", Edited by Andrew S. Gold and Paul B. Miller. First edition., Oxford University Press, 2014.
17. Grimmelman, James. "When All You Have Is a Fiduciary - LPE Project". *Law and Political Economy Project*, 2019. Accessible at <https://lpeproject.org/blog/when-all-you-have-is-a-fiduciary/>.
18. Gvelesiani, Irina. "EU Policies Regarding the Development of TrustLike Devices - Recent Challenges, Achievements, Prospects and Terminological Insights", 2016. Accessible at <https://www.econstor.eu/bitstream/10419/198447/1/ceswp-v08-i1-p093-102.pdf>

19. Hulin, Anne-Sophie. "How can civil law jurisdictions support data trusts?", 2021. Accessible at <https://datatrusts.uk/blogs/how-can-civil-law-jurisdictions-support-data-trusts-the-quebec-example>
20. Information Commissioner's Office. "Information Rights at the End of the Transition Period - Frequently Asked Questions." Guidance - Brexit FAQs - ICO, 2021. Accessible at ico.org.uk/media/for-organisations/documents/brexit/2617110/information-rights-and-brexit-faqs-v2_3.pdf.
21. "International Transfers after the UK Exit from the EU Implementation Period." ICO, 2021, Accessible at ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/.
22. Jeremiah Lau, et al. "The Basics of Private and Public Data Trusts." *Singapore Journal of Legal Studies*, no., 2020, pp. 90–114.
23. Khan, Lina M., and David E. Pozen. "A Skeptical View of Information Fiduciaries." *Harvard Law Review*, vol. 133, no. 2, Harvard Law Review Association, 2019, pp. 497–541.
24. Leblanc, J." Definition and Implementation of Data Trusts in Quebec Civil Law. Montréal: Territoires innovants en économie sociale et solidaire "2021. Retrieved from <https://tiess.ca/wp-content/uploads/2021/03/Data-Trusts-In-Quebec-Civil-Law-Synthesis-2.pdf>
25. Manohar, S., Kapoor, A., Ramesh A. " Understanding data stewardship: taxonomy and use cases", The Data Economy Lab, Aapti Institute, 2019. <https://uploads.strikinglycdn.com/files/64aa4010-6c11-4d6f-8463-efaed964d7d9/Understanding%20Data%20Stewardship%20-%20Aapti%20Institute.pdf>
26. Mari, Angelica. " Brazilian government launches data protection campaign", 2021. accessible at <https://www.zdnet.com/article/brazilian-government-launches-data-protection-campaign/>
27. Mari, Angelica." Brazilians mostly unaware of data protection regulations", 2020. accessible at <https://www.zdnet.com/article/brazilians-mostly-unaware-of-data-protection-regulations/>
28. McDonald, Sean "The Fiduciary Supply Chain", Cigionline, 2019. Accessible at <https://www.cigionline.org/articles/fiduciary-supply-chain/>
29. McFarlane, Ben."Data Trusts and Defining Property", Oxford Property Law Blog, 2019, 29, Accessible at <https://www.law.ox.ac.uk/research-and-subject-groups/property-law/blog/2019/10/data-trusts-and-defining-property>
30. Mettarlin," The Quebec trust and the civil law". *McGill LJ*, 21, 175, 1975.
<https://lawjournal.mcgill.ca/wp-content/uploads/pdf/1366082-matterlin.pdf>
31. Montgomery, Jess." Understanding the Data Governance Act : in conversation with Sylvie Delacroix, Ben McFarlane and Paul Nemitz", Data Trusts Initiative Blog, 2021.
<https://datatrusts.uk/blogs/understanding-the-data-governance-act-in-conversation-with-sylvie-delacroix-ben-mcfarlane-and-paul-nemitz>
32. OECD (2013), "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD." Available at:
<<https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonald ata.htm>>
33. OECD."Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies", OECD Publishing, 2019, Paris. <https://doi.org/10.1787/276aaca8-en>.
34. Ruhaak, Anouk "Data trusts in Germany and under the GDPR", 2020. Accessible at <https://algorithmwatch.org/en/wp-content/uploads/2020/12/Data-trusts-in-Germany-and-under-the-GDPR-Anouk-Ruhaak-AlgorithmWatch-2020.pdf>
35. SDSN TReNDS for Contracts for Data Collaboration. " Using Mobile Data For Health Monitoring: A Case Study of Data Sharing Between Ghana Statistical Services", Vodafone Ghana, and Flowminder Foundation, 2020. Accessible at <https://www.unsdsn.org/post-title61e7c848>

36. Stylianou, T." South Korea: National Assembly passes proposed amendments to strengthen data protection legislation. [online] DataGuidance", 2020. Available at:
<<https://www.dataguidance.com/opinion/south-korea-national-assembly-passes-proposed>>
37. Thomas, John and Wendehorst, Christiane (2020) "Response to the public consultation on 'A European strategy for data' ", Accessible at
https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Projects/Data_Economy/ELI_Response_European_Strategy_for_Data.pdf
38. Tuch, Andrew F."General Defense of Information Fiduciaries",2020 . Accessible at
<https://doi.org/10.2139/ssrn.3696946>
39. "UK launches data reform to boost innovation, economic growth and protect the public: Department for Digital, Culture, Media and Sport ",2021. Retrieved from https://www.wired-gov.net/wg/news.nsf/articles/UK_launches_data_reform_to_boost_innovation_economic_growth_and_protect_the_public_13092021101010?open
40. U.S. Senator Brian Schatz of Hawaii, 'Schatz Leads Group of 15 Senators In Introducing New Bill To Help Protect People's Personal Data Online",2018 Accessible at <https://www.schatz.senate.gov/news/press-releases/schatz-leads-group-of-15-senators-in-introducing-new-bill-to-help-protect-peoples-personal-data-online>.
41. "What is a Civic Digital Trust?", 2018. Retrieved from <https://marsdd.gitbook.io/datatrust/trusts/what-is-a-civic-digital-trust>
42. YIP, Man and GOH, Yihan." Navigating the maze: Making sense of equitable compensation and account of profits for breach of fiduciary duty". Singapore Academy of Law Journal, 2016, 28, 884-920. Research Collection School Of Law.