universität wien

DIGITAL TRANSFORMATIONS FOR HEALTH LAB

GOVERNING HEALTH FUTURES 2030

Putting data solidarity into practice

A guide for public and private organizations, authorities and policymakers

September 2025

This report was developed by the Data Solidarity team at the University of Vienna. It has been made possible by financial contribution from Fondation Botnar, Switzerland, to Project IMG-22-005 at Digital Transformations of Health Lab (DTH-Lab). Fondation Botnar's commitment to advancing global health is deeply appreciated, and this project would not have been possible without their contribution. DTH-Lab is hosted by Université de Genève (UNIGE), Switzerland.

Both the Data Solidarity team at the University of Vienna and DTH-Lab are committed to ensuring and enabling Global Access. The knowledge and information gained from the project will be promptly and broadly disseminated and its 'Funded Developments' will be made available and accessible free of costs and the Global Access Commitments will survive the term of the project.

Authors: Connor Hogan, Barbara Prainsack, Magdalena Eitenberger and Marlene Auer (all at the University of Vienna).

Design: Janhavi Nikharge

Acknowledgments: We are grateful to Seliem El-Sayed, Rohinton P. Medhora and Alex Stevenson for helpful comments, edits and amendments on the manuscript.

Suggested citation:

Hogan, C., Prainsack, B., Eitenberger, M., Auer, M. (2025). Putting data solidarity into practice. A guide for public and private organizations, authorities and policymakers. Geneva: Digital Transformations for Health Lab.

Date of publishing: September 2025.

Contents

Executive summary

Data, when used responsibly, has the power to transform societies, from enhancing urban planning to modernizing healthcare systems and driving innovation across industries. However, the distribution of the benefits and risks of data use remains deeply inequitable. Vulnerable communities are disproportionately exposed to risks, such as algorithmic discrimination, while powerful actors reap a disproportionate share of the benefits. On a global scale, large multinationals generate substantial profits, often without reinvesting in the communities or paying taxes in the regions that provided the data in the first place. These disparities highlight the stark power imbalances embedded in the current digital political economy, where laws and policies often favour well-resourced actors over smaller entities and individuals.

There is an urgent need for frameworks that prioritize fairness and inclusivity in the digital age. Data solidarity offers such a framework, aiming to achieve a more equitable distribution of benefits and risks in digital practices. Key to this approach is the concept of public value: the societal benefits that responsible data use can create while minimizing harm. A solidarity-based approach to data governance aims to maximize the public value emerging from the use of data and emphasizes fairness, transparency and accountability in digital practices.

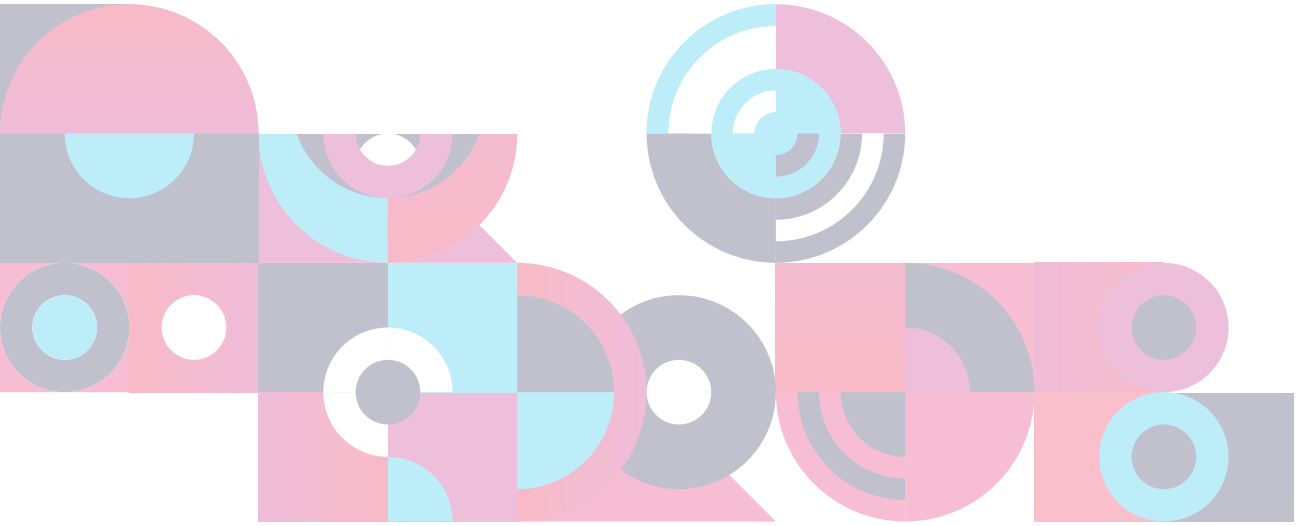
Translating these principles into action requires practical guidance. This guide serves as a tool for policymakers, businesses and civil society organizations, equipping them with strategies to implement data solidarity principles in their work. It provides actionable recommendations at all levels, introduces PLUTO (Public VaLUe Assessment TOol)[1] as a structured method for evaluating the public value of data use and explores Harm Mitigation Bodies (HMBs) as a novel mechanism for addressing data-related harms.

The structure of the guide is as follows: it begins by introducing data solidarity and the concept of public value (Section 1) before offering a step-by-step framework for putting these ideas into practice (Section 2), with tailored strategies for local policymakers, national governments, businesses and non-profits. It also discusses

[1] The PLUTO tool is available online here: https://pluto.univie.ac.at/

Harm Mitigation Bodies (HMBs) and benefit-sharing agreements (BSAs) as policy instruments to promote data solidarity by reducing harm and ensuring the benefits of data use are widely felt. Finally, the guide includes resources and further reading (Section 3).

This guide was developed within the Data Solidarity Work Programme, a multidisciplinary collaboration of researchers and policymakers led by Barbara Prainsack at the University of Vienna.[2] Since 2024, the Data Solidarity Work Programme has also been affiliated with Digital Transformations for Health Lab (DTH-Lab) led by Aferdita Bytyqi and Ilona Kickbusch.[3] The guide builds on previous publications, most notably the Data Solidarity White Paper (Prainsack et al. 2025) and the Data Solidarity Glossary (Prainsack and Kickbusch 2024).



[2] More information on the Data Solidarity Work Programme is available online here: https://datasolidarity.univie.ac.at/

[3] More information on DTH-Lab is available online here: https://dthlab.org

Key terms

The following key terms define and clarify pertinent terminology in the context of data solidarity. For further engagement the Data Solidarity Glossary (Prainsack and Kickbusch 2024) – developed within the Data Solidarity Work Programme at the University of Vienna in collaboration with Digital Transformations for Health (DTH-Lab) – provides additional insights into relevant key concepts and data solidarity's relationship to other key concepts and instruments in the domain of data governance and data ethics.

Benefits refer broadly to positive outcomes of data use. It encompasses social (e.g. giving more people access to education and information), health (e.g. improved medical treatment) and environmental benefits (e.g. improved response to climate change), among others. Benefits can be immediate and long-term, affecting future generations and can affect not only those who gave their data in the first place, but much larger groups or the whole of society.

Benefit-sharing agreements (BSAs) are a proposed mechanism to ensure that the public receives a fair share of the profits, insights, or technological advancements generated from the use of their data by private entities. By formalizing these arrangements, BSAs help balance power dynamics, promote equitable data use and ensure that those who contribute data also benefit from its commercial applications.

Data solidarity is an approach to data governance which seeks to ensure an equitable balance of the risks and benefits of digital practices.

Data use includes collecting, storing, transferring, transforming and analysing data, as well as the consequences of these actions and includes every aspect of algorithms from their design to their outcomes. This covers both the processes (like collecting user data to train artificial intelligence [AI] or analysing patient data for medical research) and the outcomes (such as a product which utilizes user data or a diagnostic tool using patient data). All these activities are relevant for assessing public value.

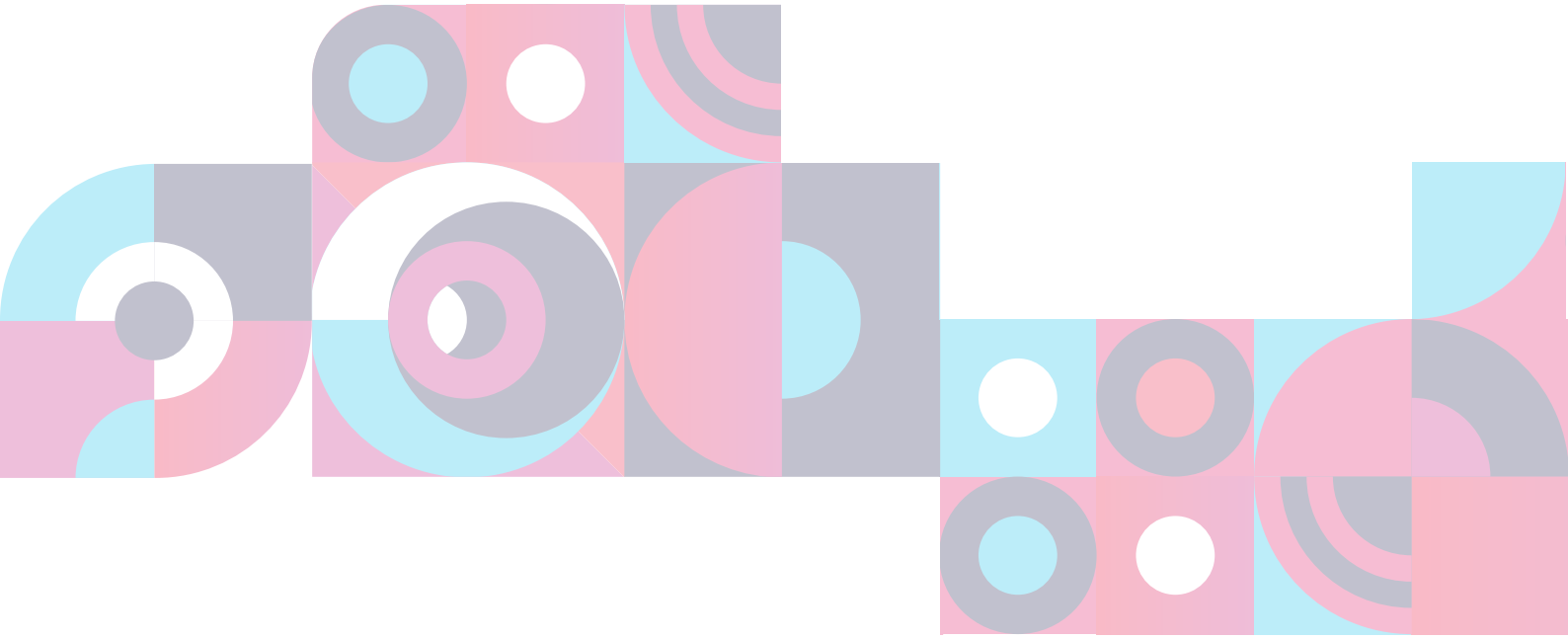
Harm refers to the negative outcomes of data use. Harm can occur both as part of the data use itself, or through the mishandling of data. It can include direct harm (such as through privacy breaches) and indirect (such as through algorithmic discrimination). Harm can occur at the individual, organizational and societal level.

Harm mitigation refers to measures in place to support those who have experienced data harm. This can take the form of, for example, an effective complaints procedure, access to independent oversight bodies, or mechanisms for correcting errors, such as the ability to contest automated decisions that have led to unfair outcomes and – in hard cases – financial support to victims of harm.

Harm Mitigation Bodies (HMBs) are proposed independent bodies that review complaints from people who claim to have been harmed by data use, but do not qualify for or cannot pursue legal remedies (see McMahon, Buyx and Prainsack 2020).

Public value refers to the value that an organization or practice contributes to society. In connection with digital data, it can be thought of as a balance between the risks and potential benefits of data use. Generally speaking, the higher the benefits and lower the risks of a given digital practice, the higher the public value. Public value is also increased when benefits and risks are distributed fairly, reducing inequalities and power imbalances and when digital practices are sustainable, ensuring value for future generations. Further, public value is increased when positive spill-over effects, or externalities, increase.

Risks refer to the potential of harm materializing through data use. For example, an instance of data use may carry informational risks, in that there is a potential for private data to be leaked. Other risks include financial risks (e.g. fraud), health risks (e.g. misdiagnosis or incorrect medical treatment as a result of mishandling) or social risks (e.g. discrimination or exclusion emerging from algorithmic biases). As with benefits, these risks can be short- or long-term, impacting not only those who gave their data but also broader groups or society at large.



1. Introduction to data solidarity

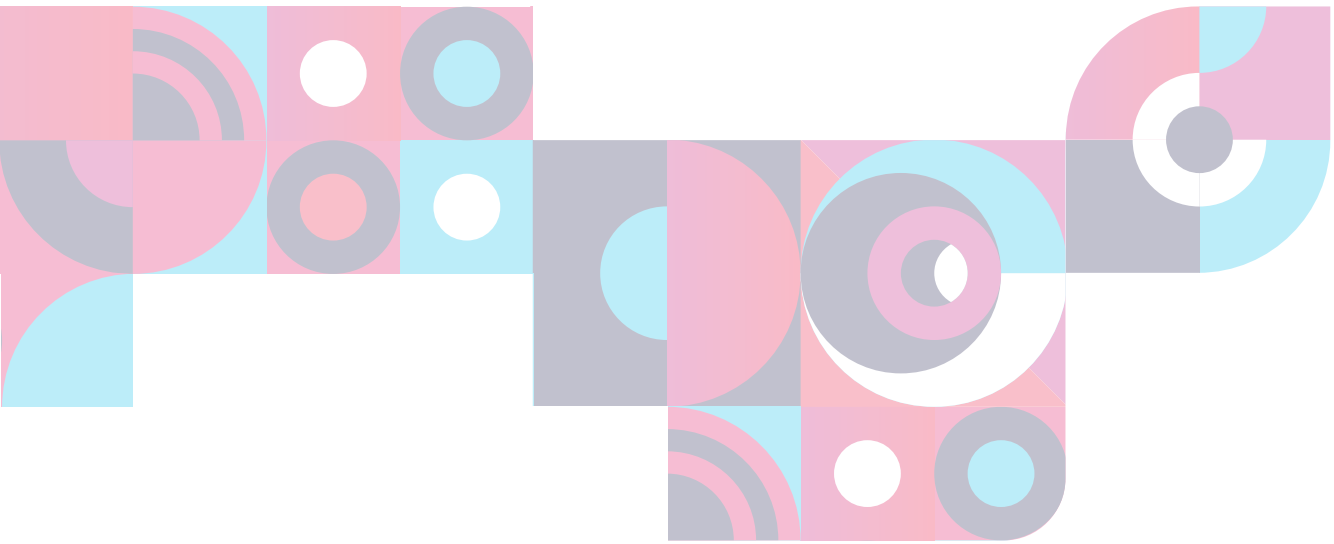
Suppose you are a policymaker in a health ministry, tasked with improving early detection of serious medical conditions across the country. You propose partnering with a private tech company to develop an app that analyses patient data (such as medical histories, blood test results and demographic information) to identify conditions like kidney disease. While the initiative enables early intervention, risks become apparent. A lack of transparency in the data-sharing agreement has left individuals in the dark about how their data is used by the private company and with whom it is ultimately shared, leading to a collapse in public trust in the app.

Now suppose you work for a private company seeking to streamline its recruiting process. You implement an AI-driven system to screen job applications and identify the best candidates based on their skills, qualifications and work history. The system analyses CVs and motivation letters submitted by applicants and ranks them against predefined criteria. While this saves time and reduces hiring costs, it turns out that algorithmic biases unintentionally disadvantage certain groups, such as women and ethnic minorities, by favouring patterns historically associated with specific demographics.

Finally, suppose you are a municipal policymaker in a major city, tasked with improving waste management and sanitation. You implement a digital waste management app that allows residents to report uncollected waste and track pickup schedules. While the app initially shows promise in affluent neighbourhoods, it becomes clear that low-income communities, where smartphone and internet access are limited, are largely excluded from the system. As a result, waste collection improves in wealthier areas but worsens in underserved neighbourhoods, exacerbating sanitation issues and local inequality.

These examples are all based on real cases (see Powles and Hodson 2017; Lagos Waste Management Authority 2021; Agbo 2023; Chen 2023)[4]. In all of them, the challenge was the same: how to balance the benefits and risks of digital practices in a fair and structured way.

Data solidarity offers a framework for addressing this challenge, ensuring that societal benefits of data use are maximized while its harms are minimized.



[4] For example, in 2014, Amazon developed a machine learning-based hiring tool that exhibited gender bias (see Chen 2023). The city of Lagos, Nigeria, has introduced a series of apps for dealing with municipal waste. However, sanitation issues in low-income areas have been exacerbated due to a lack of interest from commercial providers, worsening inequalities in waste collection (see Lagos Waste Management Authority 2021; Agbo 2023).

1.1. Data solidarity

Data solidarity is an approach to data governance that aims to balance the distribution of risks and benefits of digital practices fairly between and within societies. It aims to do this by supporting data use that brings significant benefits to the public, without exposing individuals or communities to undue risk of harm.

Realizing data solidarity requires a range of policy instruments to complement existing laws and policies. These instruments fall under three pillars (see Table 1).

Table 1: The three pillars of data solidarity (Prainsack 2017)

Pillar I	Pillar II	Pillar III
Facilitating data use that creates significant public value	Harm prevention and harm mitigation	Sharing commercial benefits with communities
E.g. via deregulation, public support for data use	E.g. via prohibiting data uses that are known to harm individuals or communities and via the establishment of Harm Mitigation Bodies	E.g. via taxes or benefit sharing agreements

Source: Prainsack & Kickbusch 2024: 7

Pillar I focuses on making those types of data use easier that promise to bring great benefits to people without posing significant risks to individual people or communities (i.e. it creates significant public value). This can be done for example by easing regulatory burdens, or by providing funding or other forms of incentives for data use with high public value.

Pillar II focuses on reducing the risk of harm and effectively prohibiting data use that poses unacceptably high risks. As not all harm can be prevented effectively, there is also the need to mitigate it when it does occur.

Pillar III seeks to ensure that some of the profits (or other commercial benefits) emerging from data use be returned to the public domain, as it is those people and communities that enabled the data use in the first place.

1.1.1. Public value

A central aspect of data solidarity is public value. Broadly speaking, public value refers to the value that an organization or practice contributes to society. Within data solidarity, public value can be thought of as a balance between the risks and benefits of data use.

From a data solidarity perspective, the goal is to maximize the public value of an organization's data use – balancing societal benefits and risks as fairly as possible. However, public value goes beyond merely calculating benefits against risks, as any data use that poses significant risks to individuals or communities precludes a positive public value score.

For instance, imagine you are a city councillor seeking to improve education in your area by initiating a digital learning platform to enhance student engagement and resource access. The platform would collect data such as students' academic performance, attendance records, learning preferences and engagement metrics. This data would be used to personalize learning experiences, identify students requiring additional support and optimize resource allocation for schools. While the initiative promises significant benefits – like improved educational coverage and targeted support – it also introduces risks such as privacy breaches and the potential misuse of sensitive information.

A structured approach is needed to assess these benefits and risks and determine when they are sufficiently balanced to proceed with the scheme. This includes considering not just the nature and extent of the benefits and risks, but how equitably they are distributed: Are there communities that might struggle to engage with the platform due to a lack of digital access, for example? Are certain populations more vulnerable to data misuse or discrimination?

Beyond weighing benefits and risks, public value is also affected by the following:

- Harm mitigation measures: Are there safeguards to address potential harm, such as mechanisms for reporting and rectifying issues?
- Transparency: Are the details of data use – such as how data is collected, what it is used for, why it is needed and who it is shared with – made clear and accessible to the public?
- Sustainability: Will the initiative deliver value over time, ensuring future generations benefit as well?

Addressing these aspects enhances public value, ensuring the initiative aligns with societal needs and fairness.

In the above example, suppose you determine that, while the potential benefits of the proposed platform are substantial, there are significant risks. These include immediate concerns, such as vulnerabilities in data storage that could expose student information to breaches and broader risks: unequal access for certain households lacking adequate internet or devices and the potential misuse of the data by third parties, leading to targeted advertising or profiling that could disadvantage specific groups of students.

More examples can be found in the following sections. Whether in a public body, a business or civil society organization, what unites them all is a focus on maximizing public value.

Once we have assessed the public value a given instance of data use is likely to generate, we can determine what "type" of data use we are dealing with, which, while being guided by the three pillars of data solidarity (see Table 1), will help us formulate a strategy to maximize public value.

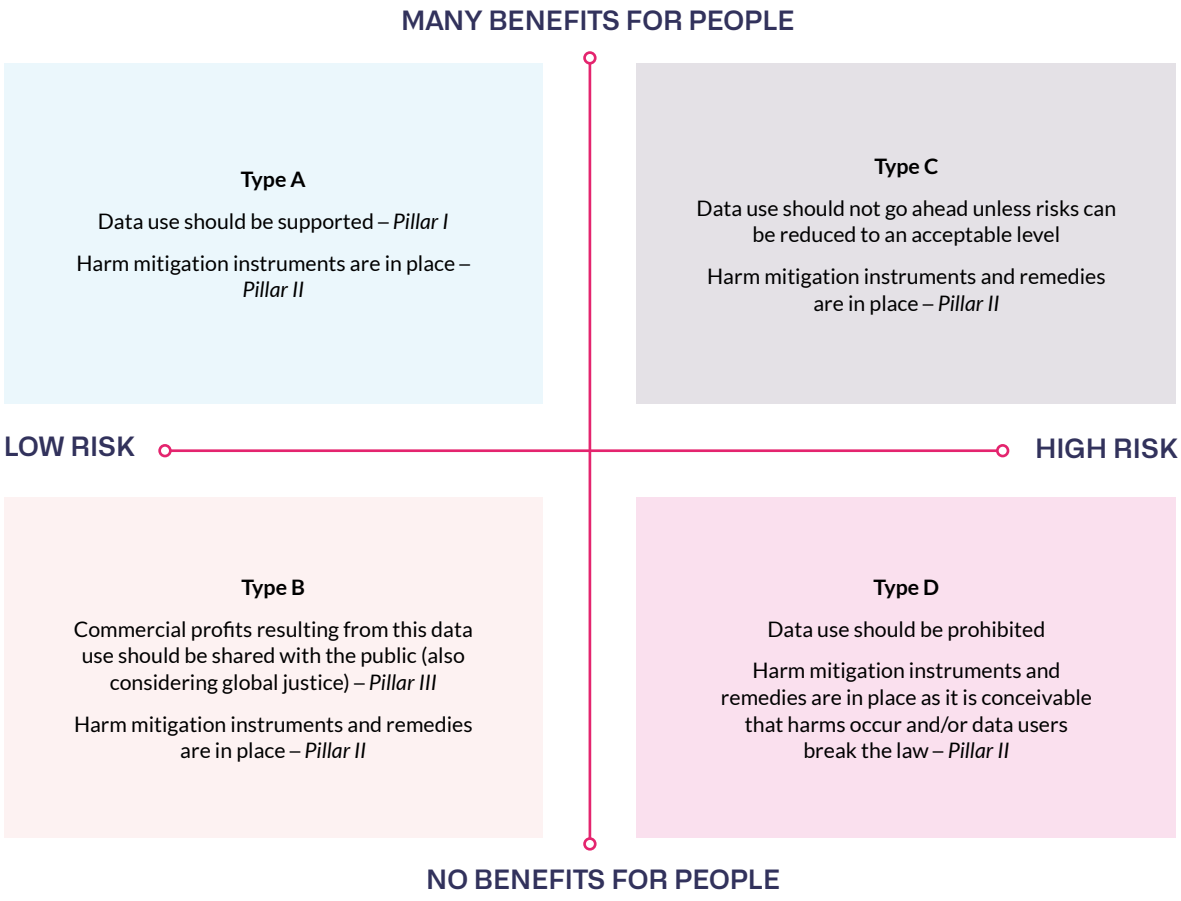
1.1.2. Types of data use

It has often been assumed that certain types of data are inherently "riskier" to use than others (such as personally identifiable versus non-personal data). Instead, data solidarity refocuses our attention to different types of data use: how is data used, by whom and for what purpose?

Within data solidarity, there are four types of data use (organized according to the plausible benefits versus risks – see Figure 1):

- **Type A:** Likely to generate significant benefits for the public and does not pose unacceptably high risks (high public value). These types of data use should be actively facilitated and promoted (Pillar I, II).
- **Type B:** Unlikely to provide significant public benefits but also poses minimal risk (potential public value). Profits from this type of data use should be partially returned to the public (Pillar II, III).
- **Type C:** Likely to generate significant benefits for the public while also posing high risks (potential public value). Should only continue if the risks are reduced to an acceptable level (Pillar II).
- **Type D:** Unlikely to provide significant public benefits while also posing high risks (low or no public value). Should be prohibited (Pillar II).

Figure 1: Types of data use within data solidarity



Source: Prainsack et al. 2025: 11

Across all types of data use, harm mitigation measures should be in place, as the risk of harm can rarely be reduced to zero (see Section 2.5 for more information on harm mitigation).

In the education scenario for instance, the platform would be considered a Type C data use (high benefits, high risks) and should not proceed until the risks are reduced to an acceptable level. This could involve measures such as enhancing cybersecurity infrastructure and ensuring low-income households are able to fully benefit from the platform.

To facilitate a structured assessment of the public value of data use, the authors have developed an online tool, which is recommended to support the evaluations outlined in this guide (see El-Sayed et al. 2023).

1.1.3. Using PLUTO

In 2023, the Data Solidarity Team at the University of Vienna created PLUTO (Public VaLUe Assessment TOol[5], El-Sayed et al. 2023) an online tool to help guide the public value assessment described here in a structured way. The tool can be used by anyone, including organizations, public authorities and policymakers who want to determine the public value that a specific instance of data use is likely to create.

PLUTO consists of just over 20 questions which cover four areas:

- Information about the data user
- Benefits of the data use
- Risks of the data use
- Institutional safeguards

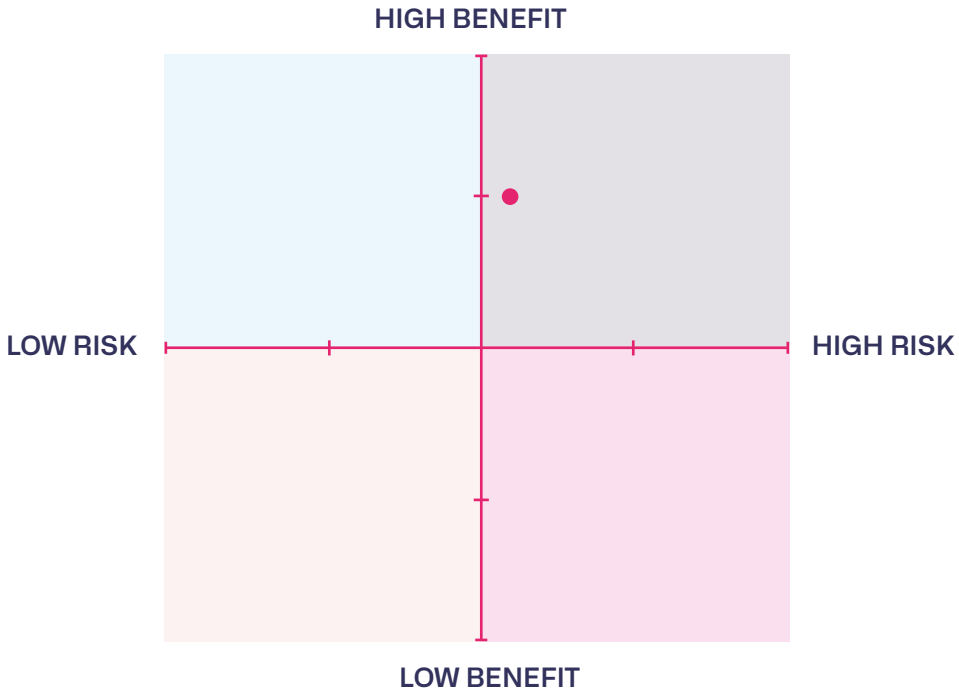
Generally, the more a specific instance of data use benefits people and communities without putting individuals or groups at risk, the higher PLUTO will score its potential public value. Benefits and harms that are likely to materialize for marginalized groups are weighted more heavily than benefits and harms for privileged groups. Additional factors such as environmental impact are also weighted.[6]

Upon completing the questionnaire, PLUTO generates a unique position in a multidimensional coordinate system (see Figure 2). This system evaluates data use based on two axes: risks and benefits. The position within this system corresponds to specific data use categories (Type A-D, see Figure 1) and suggests the appropriate changes based on the three pillars of data solidarity (see Table 1). PLUTO also produces a list of recommendations to improve the public value score of the evaluated instance of data use, based on the result.

[5] The PLUTO tool is available online here: https://pluto.univie.ac.at/

[6] Detailed information on how responses are weighted is available online on the tool's website, accessible to anyone with Internet access: https://pluto.univie.ac.at/weighting

Figure 2: Example of PLUTO results

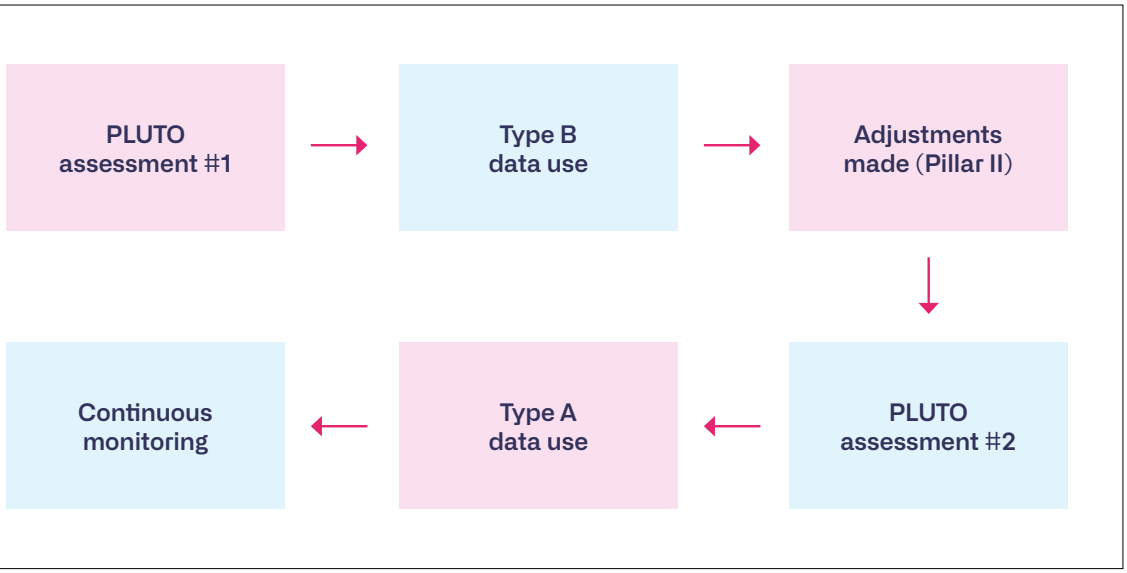


Note: In this case, the data use is Type C (high benefit, high risk). Solutions should aim at reducing the overall risk to an acceptable level.

Policymakers and organizations at all levels can use PLUTO to help streamline the process described in this guide.

See Figure 3 for an example workflow for using PLUTO and implementing its recommendations.

Figure 3: Example of improvements made in data use and data governance following a PLUTO assessment

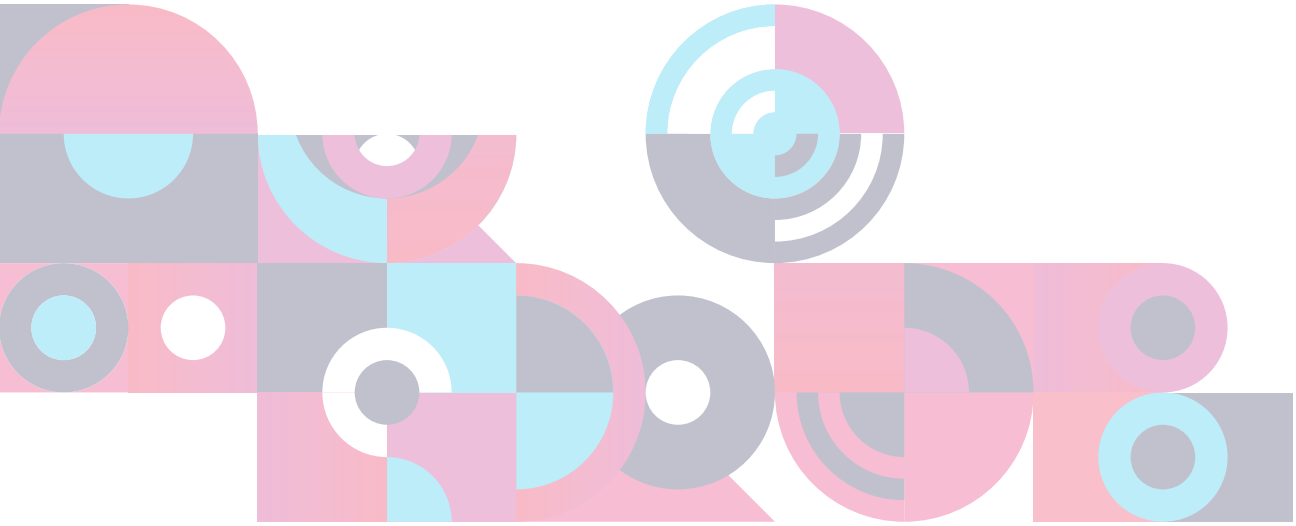


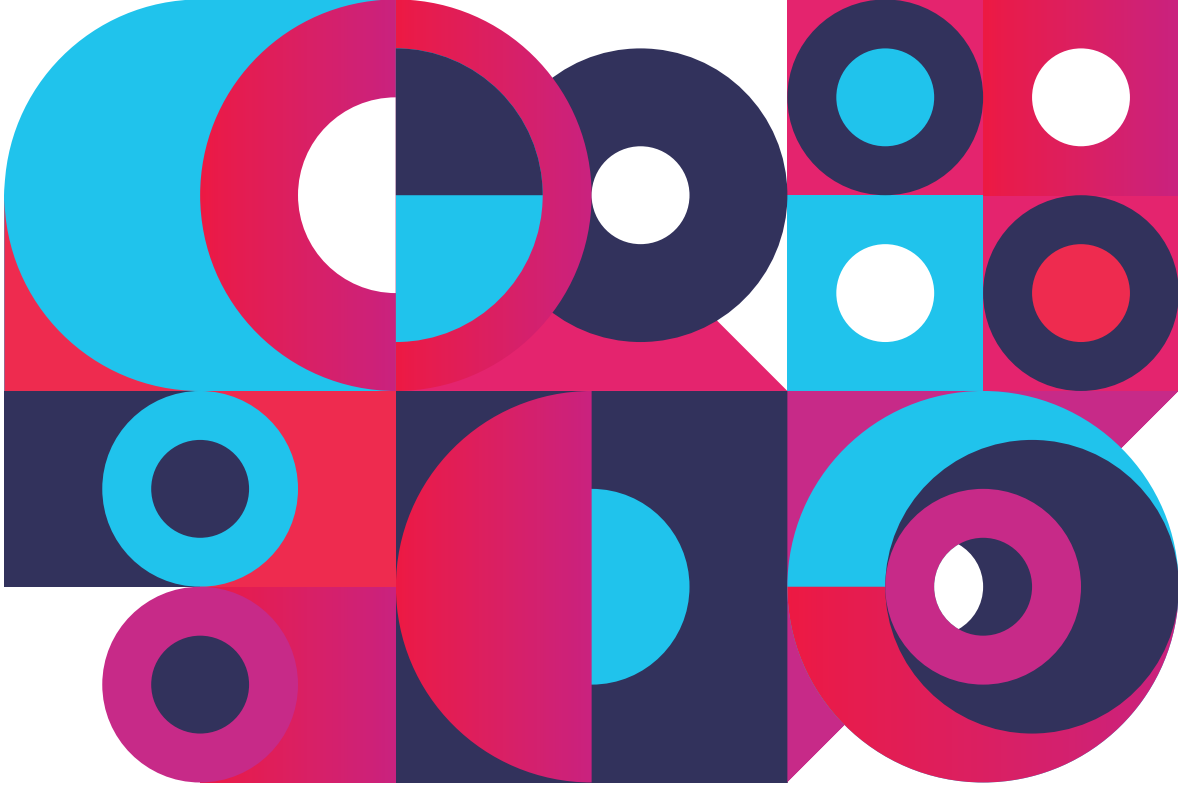
It is important to note that PLUTO does not claim to give an absolute and definitive score and should not be used as the only basis for any decision. Public value is a dynamic concept that evolves with societal changes, technological advancements and shifting values. Consequently, PLUTO's criteria and definitions may need to be updated periodically to remain relevant. Moreover, organizations and communities can tailor the PLUTO tool to their specific needs by adjusting the questions asked and the weights assigned to each question. Rather than a definitive verdict on what public value is, PLUTO aims to be a "proof of concept" prototype that shows how public value can be systematically assessed.

PLUTO is designed to function as a self-assessment instrument. Therefore, no mechanisms are provided within PLUTO to mitigate the risk of gaming or to make it "tamper-proof".

Ideally, data users would answer the questions posed in PLUTO authentically and improve their data use in accordance with the findings. However, even if actions are not taken with the intent of improving public value but for merely reputational or tokenistic purposes, we would argue that thinking through data use from a critical lens can nonetheless be an important first step towards possible future improvements.

If public bodies use PLUTO in such a way that its score unfolds legal consequences (e.g. exempting certain kinds of data use from specific regulatory requirements), suitable auditing mechanisms would need to be put in place to ensure maximum veracity and reliability of results.





2. Putting data solidarity into practice: a step-by-step guide

To put data solidarity into practice within your organization, the following steps should be taken:

1. **Evaluate the benefits and risks** associated with your organizations' data practices which together make up public value (this is referred to as the initial public value assessment). Utilizing PLUTO (see Section 1.1.3.) will aid in this evaluation.

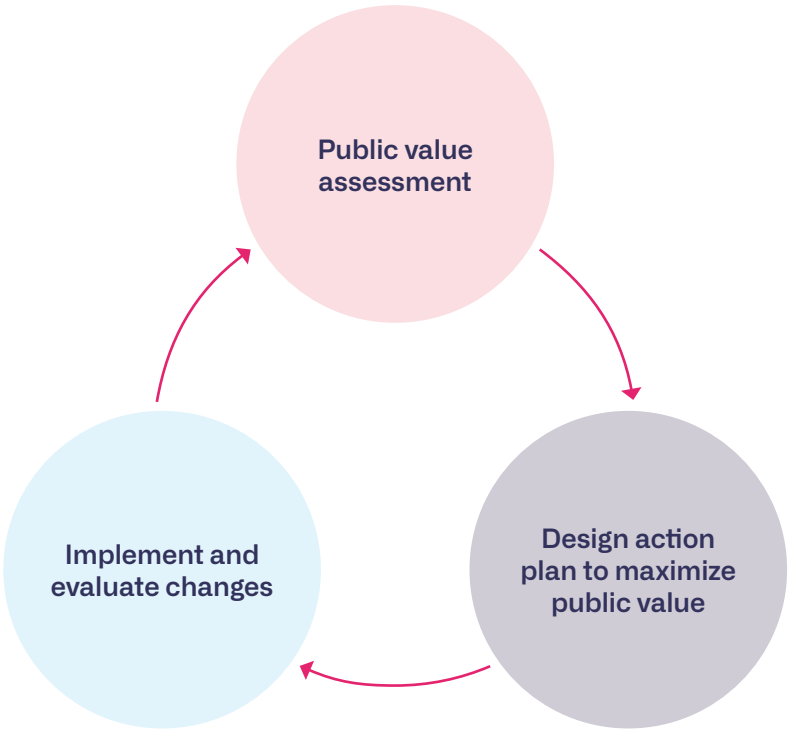
2. **Develop an action plan** to enhance the public value of your organization's data use. This plan should answer the question: "What steps can my organization take to maximize public value in its data practices?". It should clearly define the necessary policies, resources, metrics for evaluation and a timeline for implementation.

3. **Implement, monitor and evaluate improvements.** Execute the action plan and continuously track progress to ensure the organization's data practices align with data solidarity principles.

4. **Continuously monitor and adjust.** Regularly assess data use to ensure alignment with data solidarity principles and adapt to emerging risks and opportunities.

See Figure 4 for a summary of the proposed workflow.

Figure 4: Putting data solidarity into practice



The specific policies and actions recommended to maximize public value will vary depending on the needs and responsibilities of the organization or institution implementing data solidarity. A local policymaker, for example, might find that funding should be prioritized for data use which supports housing access in their area. A policymaker at the national level may find that their digital practices should be made more environmentally friendly, or that measures should be taken to reduce inequality in the provision of digital health services.

Similarly, a CEO of a large corporation may find that, to maximize the public value of their digital activities, they should invest in partnerships in low- and middle-income countries (LMICs), while a manager of a small business might focus on improving the transparency of their data practices to build customer trust. Civil society organizations, including charities and non-profits, will also have distinct priorities, such as ensuring the secure and ethical use of data from vulnerable populations, such as refugees, individuals experiencing homelessness, or communities affected by natural disasters.

What unites all these actors when seeking to adopt data solidarity in their digital practices is a shared commitment to generating public value. This means maximizing the societal benefits of digital practices, mitigating risks, reducing harms and ultimately working towards a more equitable, inclusive and sustainable digital ecosystem.

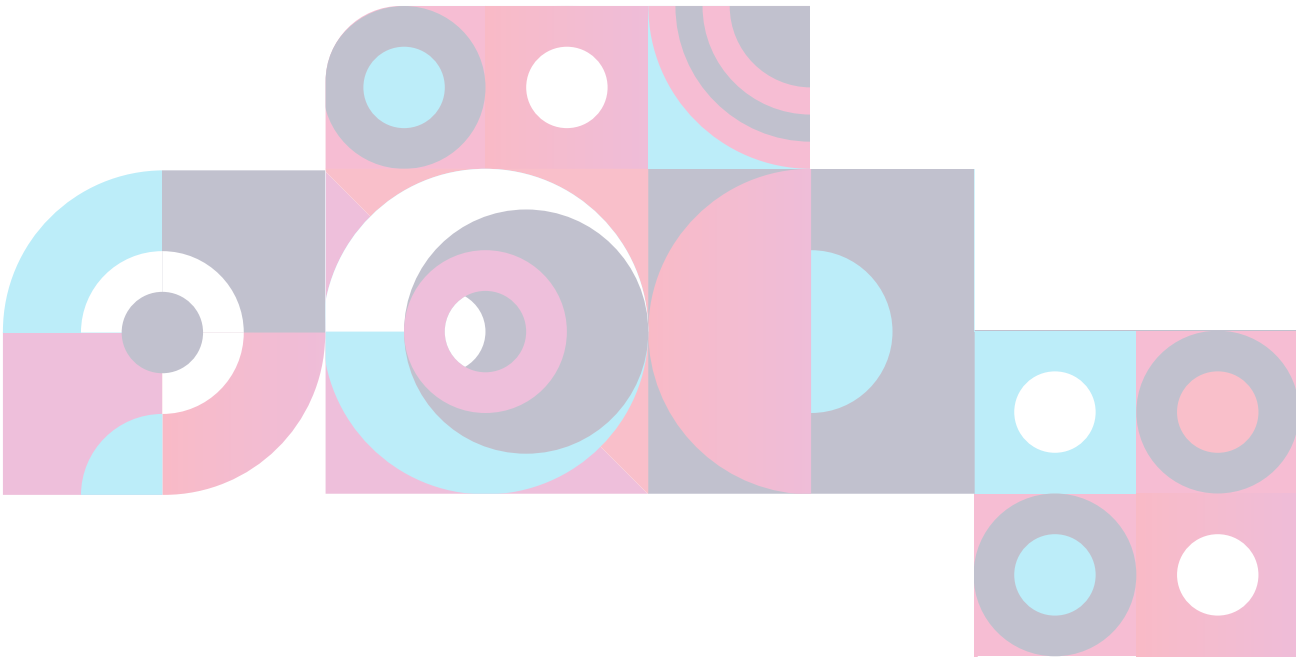
In the following sections, we offer recommendations to put data solidarity into practice at all levels: from the initial public value assessment, to structuring an action plan, to implementing and evaluating a solidarity-based policy framework. The PLUTO tool, introduced in Section 1.1.3., will support readers throughout their efforts to put data solidarity into practice.

2.1. Local and municipal policymakers

Local governments worldwide are increasingly leveraging public data to improve services and tackle modern challenges. During the COVID-19 pandemic, for instance, local and city councils used AI-powered tools to guide their responses (Allam and Jones 2020; Strielkowski et al. 2022). Today, so-called "smart cities" gather data from citizens, devices and buildings to enhance decision-making in a bid to improve quality of life.

While these kinds of data use can bring significant benefits to communities, they also carry risks. For example, the deployment of AI in areas such as housing or policing can perpetuate biases, such as racial or gender discrimination and lead to errors causing harm. In February 2024, for instance, a community worker was wrongly detained by the London Metropolitan Police due to a misidentification by their facial recognition system (Big Brother Watch 2024). Moreover, as large tech companies increasingly promote proprietary solutions for issues such as healthcare, transportation, or education at the local level, they risk side-lining local communities and deepening existing inequalities (Block 2024). The failed Toronto Quayside project illustrates how important it is to be mindful of these risks in the context of data use and the development of "smart cities" (see Box 1).

Data solidarity offers an approach for local policymakers to help balance the risks and benefits of data use while still improving the well-being, prosperity and liveability of the local environment.



Box 1: Toronto's failed Quayside project – the pitfalls of building a data-based "smart city"

In 2017, Toronto Waterfront, a government agency in charge of urban development along the Toronto waterfront, awarded the development of a 12-acre lot to Sidewalk Labs, then an urban planning subsidiary of Alphabet. The Quayside project was intended as a proof of concept for Sidewalk Labs' model of a "smart city", leveraging data-driven technologies to improve the efficiency of urban infrastructures. For this Toronto neighbourhood this included things like autonomous cars and garbage collection, heated sidewalks and the monitoring of street crossings and traffic (Jacobs 2022).

However, the project's realisation was fraught with controversies. Opponents called out a lack of transparency, both regarding the process through which Sidewalk Labs received the contract and the company's long-term plans for the development. People questioned the legitimacy of involving the private sector in the government of public urban spaces, especially a multinational like Alphabet. Residents were concerned about their privacy in an environment full of sensors collecting the data needed for the envisioned "smart" services and the governance and use of that data by a private company. It was also criticized that the proposed high-tech solutions failed to take into account people's actual needs and unnecessarily overcomplicated things. Sidewalk Labs' demands to receive a share of respective property taxes and development fees drew additional ire, as these would usually go to the city (Wakefield 2019; Jacobs 2022).

Ultimately, the project was abandoned by Sidewalk Labs in 2020, citing uncertainties that arose with the COVID-19 pandemic, but observers of the project stress the impact of the unresolved controversies that accompanied it (Jacobs 2022). Examples like Toronto's Quayside project exemplify how the risks and benefits attendant to the use of public data for urban development need to be carefully assessed and accounted for in local public policy.

2.1.1. How can local policymakers put data solidarity into practice?

2.1.1.1. Initial public value assessment

Suppose you are part of a local urban planning committee, tasked with updating your city's traffic and transport scheme to reduce congestion and identify areas where new infrastructure is needed. You decide to employ an AI model to analyse traffic data collected from various sources, such as sensors on main roads, public transport usage statistics, GPS data from ride-sharing services and satellite imagery, to identify congestion patterns, peak traffic times and frequently used routes.

From a data solidarity perspective, some key questions to consider at the start of this process include:

- **What are the potential benefits of using this data? Who stands to benefit the most?**
  Improved traffic flow, shorter journeys and better public transport will benefit commuters, businesses and the environment. However, resource allocation towards one section of the community may inadvertently disadvantage another. In 2023 for instance, the UK Government decided to invest dormant assets earmarked for community development in small towns rather than prioritizing deprived areas, raising concerns on the equitable use of resources (Weakley 2023).
- **What are the potential risks to individuals and communities?**
  Traffic data from personal devices or apps poses privacy risks if not securely managed and remains a target for hackers (Huber 2022). Mistakes can also occur, such as when a Dutch motorist was fined €380 in 2024 after an AI-powered traffic camera misidentified him scratching his head as using his phone while driving (The Jerusalem Post 2024). Additionally, AI-driven traffic initiatives may prioritize reducing congestion over enhancing public transport or sustainable mobility (Almukhalfi, Noor and Noor 2024).
- **Are there support measures in place for those who do experience harm?**
  For instance: Is there an easily-accessible complaints procedure, financial assistance or an official appeals process for people incorrectly penalized by the traffic system?
- **Are any commercial benefits shared equitably?**
  If data from the traffic management scheme generates profit (for instance, through licensing it to third parties), does the local community that provided the data in the first place benefit proportionately in return? This could be the case if some of the funds are reinvested in local community projects, for instance, and it would be crucially important to do so.

A PLUTO assessment (see Section 1.1.3.) will help guide this process. In this case, you might find that while the AI model you are considering will generate significant benefits in the form of improved traffic and transport efficiency, it could also result in reduced services for lower-income neighbourhoods. This is not to suggest that the scheme should not proceed, but rather that potential risks need to be reduced to within an acceptable level and support measures need to be in place in case harm does occur.

2.1.1.2. Developing a data solidarity action plan for local policymakers

Having carried out an initial public value assessment, you can now create an action plan detailing how to maximize public value. The plan should set out proposed policies, the resources needed to implement them, mechanisms for regular evaluation and a clear timeline.

You can structure the action plan as follows:

1. **Facilitating high public value data use**

   a. Removing barriers
   Local policymakers can streamline processes for beneficial data use by, for instance, standardizing local data-sharing agreements and creating centralized platforms for secure and efficient data access. In the example of a congestion-reduction scheme, this could include a dedicated data-sharing portal to allow traffic data to be easily accessible for public researchers and NGOs aiming to develop sustainable transport solutions or assess the environmental impact, while maintaining privacy safeguards such as anonymization and encryption.

   b. Providing support
   Local authorities should prioritize resources for data use aligned with community-specific needs. For instance, in 2016 the city of Barcelona allocated €75 million to be spent annually on digital transformation, with a focus on citizen-led, participatory democracy and technological sovereignty. This included the Decidim initiative, a civic decision-making platform which significantly increased public engagement with city politics (see Box 2).

2. **Reduce risk**
   Measures to reduce risk can include implementing robust data encryption, limiting data retention periods, regularly auditing algorithms for accuracy and bias and incorporating public feedback into system design to ensure equitable outcomes and transparency. In the case of the AI congestion-reduction scheme for example, you could mandate that areas identified as underserved are prioritized for new bus routes, offer discounted or free fares for low-income residents and conduct regular rounds of consultation with those affected. Reducing harm also means outlawing particularly harmful data practices. In the United States, cities such as San Francisco, Boston and Portland have banned police use of facial recognition technology due to concerns over biased misidentifications disproportionately impacting communities of colour (Birhane 2022).

3. **Mitigate harm**
   To help mitigate data harm when it does occur, a dedicated Harm Mitigation Body (see Section 2.5.) could be instituted as part of the scheme, which would oversee claims of harm and offer support to those affected (e.g. by reversing erroneous fines and offering financial support).

4. **Share commercial benefits**
If data partnerships with private transport companies yield financial gains, local authorities could reinvest these funds into community programs, such as improving public transport infrastructure, subsidizing travel costs for low-income residents, or supporting local education and healthcare initiatives. A benefit-sharing agreement between the local council and private transport companies (see Section 2.6.) would create a formal mechanism to ensure that a portion of the profits generated from data use is reinvested into the community.

5. **Resource the necessary changes**
You might establish a dedicated team or appoint an individual within your organization to oversee the action plan. Smaller bodies might collaborate with regional agencies or consultants to address capacity gaps. Securing stakeholder buy-in is essential and could be achieved through public consultations, participatory workshops and clear communication of the plan's societal benefits.

6. **Evaluate measures**
Regular evaluation ensures the action plan remains aligned with community needs and data solidarity principles. For the above example, local policymakers could conduct quarterly reviews to assess metrics such as reductions in commute times, feedback from residents in underserved areas and environmental benefits like emissions reductions. Engaging affected communities directly, such as holding town halls or soliciting surveys, ensures that policies continue to address inequities and meet public needs. For example, Amsterdam and Winterthur are "smart cities" that have enhanced quality of life by engaging citizens directly in data initiatives and providing accessible data infrastructures for better services and informed participation (Neuroni et al. 2019).

Box 2: Barcelona – promoting public value through collective decision-making

From 2015 to 2019, under the leadership of progressive city officials, Barcelona launched a series of initiatives that aimed to leverage public data to shift control from private interests to civic movements and communities, most notably: Decidim Barcelona (Charnock, March and Ribera-Fumaz 2021; Monge et al. 2022).

Decidim (which is Catalan for "we decide") is an open-source platform empowering citizens to contribute to decisions such as budget allocations and urban planning, decentralizing power and fostering collective decision-making. In March 2018, the platform had over 28,000 registered participants, facilitated 821 public meetings and resulted in 12,173 proposals, of which 8,923 were incorporated into public policy (ibid.). This included the collective drafting of a citywide plan to reduce air and noise pollution and the volume of city traffic through the construction of urban superblocks which prioritize open, shared, green public spaces.

By prioritizing collective decision-making and the empowerment of ordinary citizens, Barcelona's city officials have enhanced public value while reducing power asymmetries between governments, private entities and the public.

2.2. National policymakers

Data has the potential to revolutionize public services and improve the quality of life for citizens. For example, in several countries, national telehealth policies have expanded remote healthcare services, allowing patients – particularly those in rural areas and the elderly – to more easily access medical consultations and resources (Rush et al. 2022). However, some clearly beneficial data uses, such as groundbreaking scientific research, are sometimes hindered by bureaucratic red tape, slow approval processes and restrictive data-sharing policies, limiting their potential impact (Donaldson and Koepke 2022).

Moreover, national policymakers must also contend with risks like algorithmic bias, privacy breaches and exclusionary practices. For instance, while digital solutions enabled children's' education to continue during the COVID-19 pandemic, not all families had the social or technological resources needed to benefit from them (Greenhow, Lewin and Staudt Willet 2021). A stark illustration of the risks attendant to data use at the national level is the Dutch childcare benefits scandal, in which a self-learning algorithm caused widespread harm by wrongly labelling parents as having made fraudulent welfare claims (see Box 3). National policymakers can also use other avenues, such as equitable taxation policies and participation in regional and global discussions on data governance.

Box 3: The risks of automated systems – the childcare benefits scandal in the Netherlands

In January 2021, the Dutch government resigned following a childcare benefits scandal in which a self-learning algorithm wrongly labelled over 20,000 parents – disproportionately those with immigrant backgrounds – as having made fraudulent benefit claims. The tax authority's "self-learning" tool systematically flagged benefit claims from families holding dual citizenship as high risk, triggering severe repercussions. A report by the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) showed that parents were forced to repay substantial sums, leading to financial ruin and severe emotional distress (Autoriteit Persoonsgegevens 2020). An investigation by the Dutch Data Protection Authority later revealed that bias had crept into the algorithm's design, skewing its outputs against vulnerable populations. Although human officials were ultimately responsible for determining fraudulent claims, their heavy reliance on the algorithm magnified these biases (ten Seldam and Brenninkmeijer 2021).

The scandal put a spotlight on how errors in automated enforcement can spiral into large-scale, society-wide harms, particularly when governance structures are weak. It also underlined the complexity of tracing the root causes of algorithmic bias, highlighting the need for proactive oversight, transparency and accountability (ibid.).

2.2.1. How can public policymakers put data solidarity into practice?

2.2.1.1. Initial public value assessment

Imagine you are part of a national health ministry tasked with improving patient outcomes and reducing healthcare disparities. You propose creating a secure, centralized platform for electronic patient records from hospitals, clinics and primary care providers nationwide, enabling authorized stakeholders to track disease patterns, identify resource gaps and implement targeted public health measures.

You might consider the following benefits and risks as part of the initial public value assessment:

- **What are the potential benefits of using this data? Who stands to benefit the most?**
  Centralizing patient information can reduce duplication of tests and treatments, speeding up referrals and improving care quality. Patients, healthcare providers and under-resourced regions could stand to benefit the most from these efficiencies.
- **What are the potential risks to individuals and communities?**
  Large-scale data storage raises cybersecurity concerns. The example of the 2018 SingHealth data breach in Singapore, where a well-resourced cyberattack compromised the personal data of 1.5 million patients, underscores the severity of risks faced by national healthcare systems (The Straits Times 2018). Additionally, if clinics or communities in certain areas are not covered, policy decisions could exacerbate existing health inequalities.
- **Are there support measures in place for those who do experience harm?**
  Consider: What recourse do individuals or communities harmed by your data use currently have? Effective complaints procedures, free legal assistance and appeals processes are among the mechanisms that can help provide support to individuals and communities when harm does occur as a result of the data use.
- **Are any commercial benefits shared equitably?**
  If data partnerships with private actors generate profits, are some of these reinvested into the communities whose data made them possible? For example, by making any insights gained from data analytics publicly accessible, or by progressively taxing large data-driven companies.

A PLUTO assessment (see Section 1.1.3.) will help structure this evaluation. In this scenario, although consolidating health data holds substantial promise, it also brings risks that need to be managed. This doesn't imply the project should be shelved; rather, robust safeguards, inclusive planning and clear accountability measures must be in place to ensure the initiative is truly valuable for the public.

2.2.1.2. Developing a data solidarity action plan for national policymakers

Following the initial public value assessment, create an action plan to maximize the value emerging from the public body's digital activities. This plan should clearly outline proposed policy instruments, the resources needed to implement them, a mechanism for regular evaluation and a realistic timeline.

You can structure the action plan as follows:

1. **Facilitating high public value data use**

   a. Removing barriers

   You could simplify or remove unnecessary barriers to data use with a high public value by streamlining approval processes, standardizing data-sharing protocols and clarifying legal requirements. For example, New Zealand's Integrated Data Infrastructure (IDI) reduced bureaucratic hurdles for researchers and public bodies by providing secure access to linked, anonymized data from across government agencies (Jones et al. 2022; Statistics New Zealand 2022). This system has supported evidence-based decision-making in public health, education and social services while maintaining strong privacy safeguards. Similarly, India's Ayushman Bharat Digital Mission has streamlined health data interoperability, allowing public bodies and researchers to securely access and use anonymized health records (National Health Authority 2023; Sharma et al. 2023).

   b. Providing support

   Data use with significant public value can be encouraged through targeted financial incentives, grants, or preferential access to services or datasets. For instance, governments could offer subsidies to projects that use health data to develop innovative treatments or improve healthcare accessibility. In the case of a centralized health platform, providing grants to hospitals for adopting interoperable systems could ensure equitable participation and maximize public benefit.

2. **Prevent harm by reducing risk**

   Minimizing risks to individuals and communities from data use requires proactive measures such as regular, independent audits of public data systems and the introduction of policies that address emerging threats, like mandatory data encryption standards or regulations against discriminatory algorithmic practices. For example, Canada's Artificial Intelligence and Data Act includes provisions to mandate that high-impact AI systems meet standard requirements with respect to safety and human rights (Government of Canada 2023).

   Additionally, banning harmful activities, like Norway's ban on manipulative social media images (see Box 4), demonstrates how regulation can prevent societal harm from data use.

Mitigate harm
Support should be available for individuals and communities harmed by data use, whether directly or indirectly. For a public body, these supports could include accessible complaint mechanisms, free or subsidized legal assistance and financial compensation (see Porter 2019)[7]. A dedicated Harm Mitigation Body (see Section 2.5.) could be established at the national level – or within individual public bodies – to collect information on data harms, assess cases and dispense support (financial or otherwise) to those affected.

Share commercial benefits
If data partnerships with private actors generate profits, public policymakers should aim to ensure that a portion of these – and any other related benefits – is reinvested in the communities whose data enabled them in the first place. This could be achieved through formalized benefit-sharing agreements between institutions (e.g. hospitals or universities) and private partners, which would require partial community reinvestment as a condition for data sharing (see Section 2.6.). Additionally, policymakers may consider progressive taxation at the national level; for instance, France's Digital Services Tax obligates large tech companies benefiting from citizens' data to contribute back to public funds (BBC 2019).

3. **Resource the necessary changes**
Establish a dedicated team within your organization to oversee the implementation of the action plan and ensure alignment with data solidarity principles. Smaller agencies or departments could collaborate with academic institutions or other partners to address expertise or resource gaps.

4. **Evaluate measures**
Regular evaluation is essential to monitor the initiative's progress and align it with public value. From a data solidarity perspective, it is vital to evaluate both benefits and risks, as well as their distribution. In the example case, metrics could include reductions in wait times, improved diagnostic accuracy and increased healthcare accessibility in underserved areas. Transparent reporting, such as publishing quarterly reviews in accessible formats, builds accountability and trust.

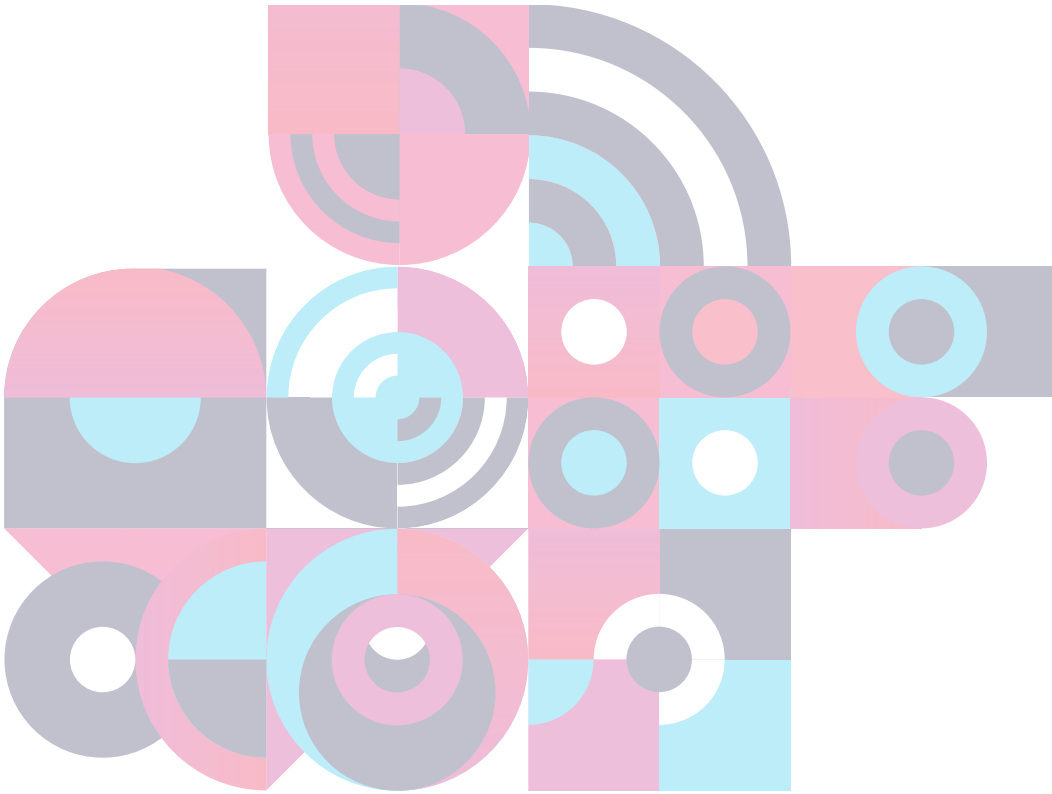
Policymakers should also engage directly with communities, seeking feedback to identify barriers and refine the initiative. For example, consultations with rural healthcare providers could reveal infrastructure gaps, while discussions with advocacy groups might suggest ways to address privacy concerns.

[7] A notable example is the 2017 Equifax data breach, where the personal information of nearly 148 million consumers was compromised. In response, the United States Federal Trade Commission mandated a $700 million settlement (amounting to up to $20,000 per person affected), demonstrating how legal frameworks can hold organizations accountable and provide restitution (see Porter 2019).

Box 4: Norway's ban on manipulative social media images

In June 2021, Norway introduced legislation requiring social media posts to carry clear disclaimers if they feature digitally altered images (Hutchinson 2021). This measure targets content where body shapes, skin tones, or facial features have been manipulated to create unrealistic appearances – an increasingly common practice among influencers and advertisers. The ban seeks to combat harmful body-image standards, particularly among younger users, by fostering greater honesty in digital marketing and self-presentation. Violations may lead to fines or legal consequences.

Examples such as these demonstrate how targeted national legislation can reduce risk by ensuring that data-driven practices do not mislead the public or compromise individual and collective well-being.



2.3. Businesses

Across the globe, businesses are generating significant profits by leveraging data in innovative ways. For example, companies in sectors such as retail and finance use consumer data to personalize services, enhance marketing strategies and optimize supply chains, driving growth and efficiency. However, the use of data also introduces risks for businesses and the individuals and communities they serve. These can include privacy breaches that undermine customer trust and algorithmic biases that could lead to discriminatory practices. In 2020 for example, it was discovered that Uber and Lyft's pricing algorithms charged higher fares in predominantly non-white neighbourhoods in Chicago (see Box 5), highlighting systemic biases in algorithmic decision-making and badly affecting public trust.

Data solidarity provides a framework for businesses to balance these benefits and risks, aligning their practices with societal good while remaining profitable. By prioritizing public value, companies can boost public trust and create products and services that benefit both users and broader society.

Box 5: Algorithmic bias in ride-hailing pricing: Uber and Lyft

In 2020, researchers from George Washington University analysed over 100 million ride-hailing trips in Chicago, comparing pricing data from Uber and Lyft against demographic statistics (Lu 2020; Pandey and Caliskan 2020; for more examples see Akter et al. 2022). They discovered that rides beginning or ending in neighbourhoods with predominantly ethnic minority populations consistently incurred higher per-mile costs than those in predominantly white areas. These pricing disparities occurred even in the absence of increased demand, suggesting systemic biases embedded in the algorithms.

The study highlighted how structural racism, such as historical redlining and geographical segregation, influences algorithmic decision-making. Although the algorithms did not explicitly consider race, factors tied to neighbourhood characteristics, such as median income or housing prices, indirectly perpetuated racial inequalities. This resulted in financial discrimination, disproportionately affecting communities of colour, who were already more likely to face economic disadvantages.

From a data solidarity perspective, this case illustrates the risks of uncritically adopting algorithmic systems without safeguards to address biases and ensure equitable outcomes.

2.3.1. How can businesses put data solidarity into practice?

2.3.1.1. Initial public value assessment

Suppose you are part of a company developing a fitness app that collects health data – such as heart rate, activity levels and sleep patterns – from wearable devices. The app uses this data to provide users with personalized fitness recommendations and track progress. Users benefit from these innovations, but may also be exposed to risk, for example if their personal data is not handled securely or if it is used for purposes they did not originally consent to.

Below are key questions to guide the initial public value assessment:

- **What are the potential societal benefits of using this data and who stands to benefit most?**
  Individual users could experience improved fitness outcomes and healthier lifestyles through personalized recommendations. On a broader scale, anonymized data shared with researchers could uncover valuable insights into population health trends, informing public health policies and interventions. However, these benefits may be unevenly distributed if access to wearable devices or app subscriptions remains limited to wealthier demographics, exacerbating health disparities.
- **What are the potential risks to individuals and communities?**
  Data breaches could expose users to risk of harm, for example through identity theft. In 2018 for instance, the fitness app MyFitnessPal experienced a significant data breach, compromising personal information for millions of users and exposing them to significant risk of fraud (Baker 2021). Additionally, if shared with third parties, such as insurers, user data could be used to increase premiums for specific populations, further entrenching social inequality.
- **Are there support measures in place for those who do experience harm?**
  At a minimum, users should have access to an effective and easily-accessible complaints procedure for when harm occurs as a result of the app's data use. Additional support measures might include a dedicated helpline or online chat for resolving issues or an appeals process to review and rectify unfair outcomes.
- **Are any commercial benefits shared equitably?**
  Consider: If the app generates significant profits, are those benefits shared with the communities whose data made them possible? For example, does the company reinvest in local initiatives, fund community programs, provide subsidies to underserved users or pay its fair share of taxes and not use tax havens?

2.3.1.2. Developing a data solidarity action plan for businesses

Having completed a public value assessment of your company's data use, the next step is to develop an action plan to maximize that value by promoting beneficial data use, reducing risks and mitigating harm. This plan should clearly outline proposed actions, the resources needed to implement them, a mechanism for regular evaluation and a concrete timeline.

You can structure the action plan as follows:

1. **Facilitating high public value data use**
   Consider how your business can better facilitate beneficial data use by actively diverting resources or creating incentives that align with societal needs. For example, if your fitness app collects anonymized health data, you could share insights with researchers working on public health projects or partner with local governments to design wellness programs for underserved communities. Offering discounted or free app subscriptions to low-income users is another concrete way to ensure broader access to the benefits your product provides.

2. **Reduce risk**
   Minimizing risk requires proactive measures such as advanced encryption, regular audits of data systems and privacy impact assessments. Systemic safeguards, such as implementing fairness checks in AI systems, can help address discrimination and equity concerns. Additionally, public commitment to refrain from engaging in harmful data practices (such as promoting hateful content to drive social media engagement) can reduce risk and boost trust.

   Additionally, banning harmful activities, like Norway's ban on manipulative social media images (see Box 4), demonstrates how regulation can prevent societal harm from data use.

3. **Mitigate harm**
   To ensure those affected negatively by data use are adequately supported, businesses must go beyond meeting legal requirements and institute proactive measures. Affiliating with an independent ombudsman or establishing an internal Harm Mitigation Body (see Section 2.5.) can provide a formal avenue for addressing data harm when it occurs as a result of your business' data use.

   At a minimum, complaints procedures and helplines should be easily accessible and responsive, ensuring users can report issues promptly and receive timely resolutions. They should also provide clear communication to users and citizens about the steps taken to address the harm, include an appeals process for unresolved cases and offer transparency in how complaints are handled to build trust and accountability. Timely, clear and consistent information on the nature of the breach and its likely impacts are crucial to decrease potential negative consequences of incidents.

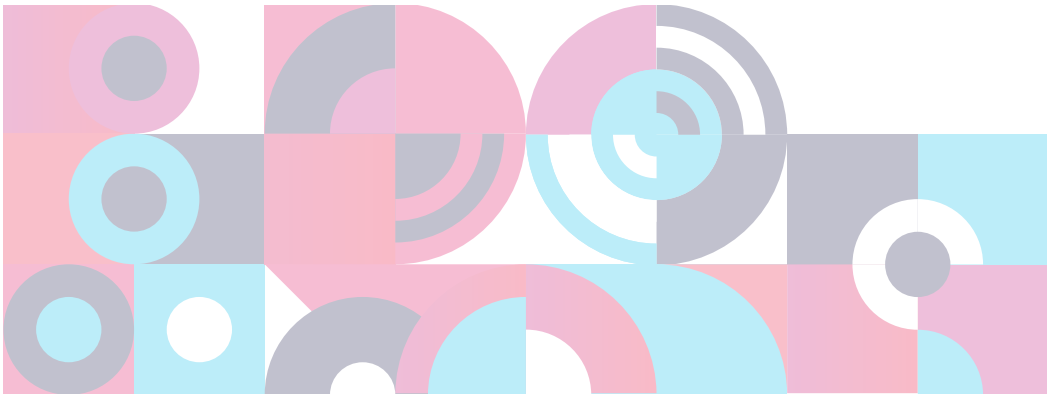
   Beyond Harm Mitigation Bodies, transparency in operations and clear communication regarding negative consequences of data use should also feature in sections on local and national government.

Share commercial benefits
If your data use generates significant profits, some of these benefits should be reinvested in the communities that provided the data in the first instance. For example, some companies in the pharmaceutical sector reinvest profits into health programs in lower- and middle-income countries (LMICs), providing affordable medicines and supporting local healthcare infrastructure (Leisinger, Garabedian and Wagner 2012). In the example case, your app could follow a similar approach by funding fitness initiatives in LMICs, or sharing insights with local organizations geared at reducing inequality. Strava, a fitness tracking app, demonstrates this ethos by sharing anonymized heat maps with urban planners and researchers to design safer and more efficient cycling and pedestrian infrastructure (Strava Support 2024). Entering into a formal benefit-sharing agreement (see Section 2.6.) with public partners can help foster long-term social impact and public trust in your company.

4. **Resourcing**
Larger companies should appoint a dedicated employee or team to oversee the action plan's implementation, while smaller organizations could consider outsourcing to experts in data ethics. To ensure buy-in, it is crucial to engage the entire company in the data solidarity process. This could be achieved for example through internal workshops, roundtables and open discussions, fostering awareness and collaboration across all levels of the business.

5. **Evaluation**
Regular evaluation is essential to ensure your action plan remains aligned with data solidarity. For the fitness app, this might include quarterly reviews of user engagement, feedback on privacy features and impact assessments of community-focused initiatives. Metrics like retention rates, satisfaction surveys and community health outcomes can provide valuable insights. Publishing these findings in accessible formats will demonstrate transparency and help maintain user trust.

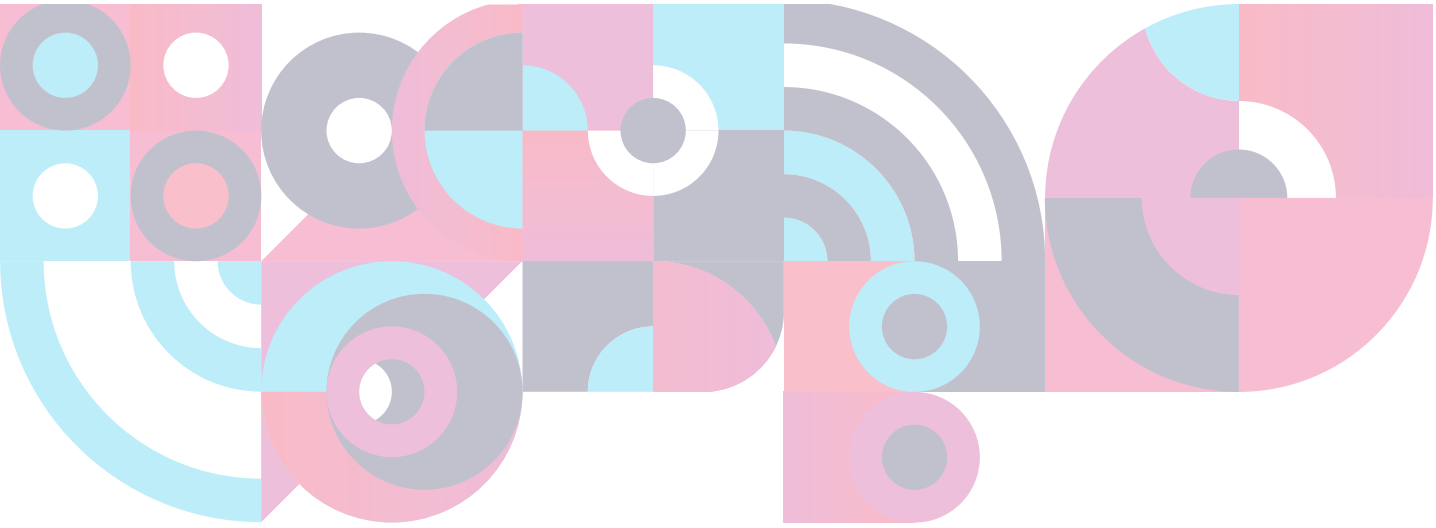
Continually consulting individuals and communities is also critical to refining your business' approach. For example, gathering input from users in deprived areas can help identify barriers to access, while engaging with local advocacy groups may provide insights into improving the public value of your data use. CoGo, a small app that tracks individual carbon footprints, exemplifies this by incorporating user feedback to refine its features in societally beneficial ways (see Box 6).



Box 6: CoGo – community engagement and sustainability

CoGo, a data platform that helps users track and reduce their carbon footprints (https://www.cogo.co/), demonstrates how businesses can integrate community input into their operations to ensure they are maximizing public value (Fahey 2021). The platform integrates with banking services, using anonymized transactional data to calculate the carbon emissions of user purchases. For example, CoGo partnered with NatWest to develop a carbon tracker embedded in a banking app, allowing over 300,000 users to measure and reduce their carbon footprints. It also highlights businesses that adhere to ethical practices, such as paying a living wage, reducing waste, or donating to environmental causes.

CoGo actively incorporates community input by enabling users to communicate their values directly to businesses through the app. When users make purchases, they can send messages to business owners about the social and environmental issues they care about, fostering a dialogue that encourages businesses to align with consumer values. This feedback mechanism empowers consumers and helps businesses understand and respond to the ethical preferences of their customer base (see Goodstack undated). By combining actionable insights with a focus on transparency and accountability, CoGo exemplifies how businesses can use data to promote societal and environmental benefits while fostering trust and consumer engagement.



2.4. Charities and non-profits

Charities and non-profits often rely on data to advance their missions, whether for identifying community needs, allocating resources efficiently, or measuring program effectiveness. For example, Médecins Sans Frontières (MSF) uses health data collected during its operations to track disease outbreaks and improve its response to humanitarian crises, while UNICEF leverages data to monitor child welfare indicators, such as vaccination rates and education access.

However, using data to assist vulnerable populations also presents elevated risks. In 2022 for instance, the mental health charity Crisis Text Line faced criticism after sharing anonymized user data with an AI company to streamline its services, raising concerns about whether those experiencing a mental health crisis could give meaningful consent to share their data (BBC 2022).

To navigate these challenges, data solidarity offers a structured framework that empowers charities and non-profits to use data responsibly, ensuring that the societal benefit of their activities is fully realized while also safeguarding individuals, reducing risks and promoting equity in their data practices.

2.4.1. How can charities and non-profits put data solidarity into practice?

2.4.1.1. Initial public value assessment

Suppose your non-profit is working to improve education access for underprivileged students. To support this, you develop a platform that collects data on school attendance, internet connectivity and learning outcomes. The data is sourced from surveys, local education departments and publicly available datasets to identify areas where students face the most significant barriers to education, such as inadequate infrastructure or limited teacher availability.

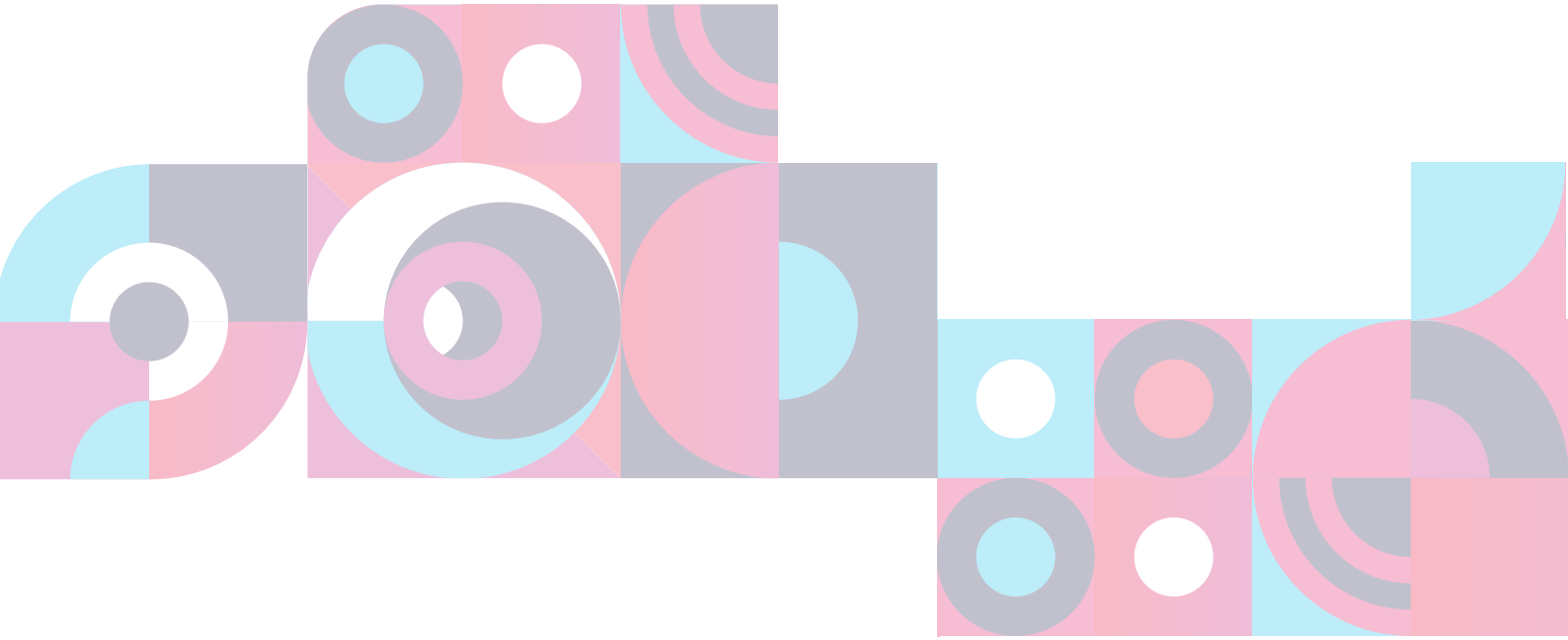
Key questions to guide the assessment:

- **What are the potential benefits of using this data and who stands to gain the most?**
  The platform could help direct resources like learning materials, teacher training and digital infrastructure to schools in high-need areas. Students in remote or low-income communities could gain access to quality education, while teachers might benefit from targeted professional development programs. Consider which communities (e.g. rural, low-income) might be inadvertently excluded, for example by lacking an internet connection.

- **What are the potential risks to individuals and communities?**
  Data breaches could expose sensitive information about students, such as socioeconomic status or academic performance, leading to stigma or discrimination.
- **Are there support measures in place for those who do experience harm?**
  For example, is there a complaints mechanism for families or schools that feel excluded or negatively impacted by the program? A hotline or digital portal could allow affected parties to raise concerns.
- **Are any commercial benefits shared equitably?**
  If the platform's anonymized data is shared with private partners for educational research or technological development, is part of the revenue reinvested into the schools and communities providing the data?

  Note: While some charities and NGOs do not cooperate with private partners, if they do, revenue-sharing is a crucial step towards data use in line with data solidarity, provided community initiatives are not already their main method of operation.

Utilizing PLUTO (see Section 1.1.3.) will help structure the initial assessment. In this instance, your analysis might reveal that while urban schools benefit significantly from the initiative, rural schools face challenges due to unreliable internet access. The charity should therefore prioritize addressing these disparities to ensure equitable access and maximize the initiative's impact.



2.4.1.2. Developing a data solidarity action plan for charities and non-profits

Having completed the initial public value assessment, develop an action plan to maximize public value of your organization's data use. This plan should clearly outline proposed actions, the resources needed to implement them, a mechanism for regular evaluation and a concrete timeline.

You can structure the action plan as follows:

1. **Facilitating high public value data use**
   As a charity or non-profit, your organization's mission is more than likely already aligned with the generation of public value. However, this can be increased by using data strategically to maximize benefits and minimize risks. For example, a homelessness charity could analyse shelter occupancy and weather data to prioritize emergency housing, while an education non-profit could use learning analytics to target struggling schools with additional resources.

2. **Reducing risk**
   Charities and non-profits often handle data from vulnerable communities, making responsible data management essential. This includes practices such as anonymizing sensitive information whenever possible, ensuring secure data storage and enforcing strict data-sharing protocols. The Red Cross and Red Crescent Societies exemplify ethical data handling in humanitarian work, prioritizing secure and responsible management of sensitive information (see Box 7).

3. **Mitigating harm**
   This can include clear procedures for addressing complaints, offering support to those harmed by data practices, or collaborating with external Harm Mitigation Bodies (see Section 2.5.). Partnering with local or national governments or likeminded advocacy groups can also help mediate issues and ensure accountability in data use.

4. **Sharing commercial benefits equitably**
   If the platform's anonymized data is shared with private partners for educational research or technological development, ensure that part of the revenue is reinvested into the schools and communities providing the data, perhaps by making it a necessary condition for data access as part of a benefit-sharing agreement (see Section 2.6.). In the example case, funds could be used to set up computer labs, subsidize internet costs for underprivileged students, or to fund educational initiatives in LMICs. If a charity or non-profit already uses community initiatives as its main method of operation, no additional steps are necessary, but a reflection on benefits sharing can nonetheless be a helpful step.

5. **Resourcing**
   Larger organizations might dedicate staff to oversee the implementation of data solidarity in their work, while smaller non-profits could consider pooling resources through partnerships or sector-specific data solidarity networks. Staff and volunteers could also be trained on data solidarity principles to ensure continued alignment with ethical practices and organizational goals.

6. **Evaluation**
Regular evaluation allows organizations to assess the effectiveness of their data practices and ensure alignment with community needs. For instance, a non-profit addressing homelessness might track metrics such as the number of individuals housed, the long-term stability of placements and service user feedback. It is vital from a data solidarity perspective to evaluate both benefits and risks, as well as their distribution. Relevant metrics could include demographic equity in service reach and user satisfaction, collected through feedback forms, surveys and focus groups.

Box 7: Ensuring ethical data management in humanitarian work: the Red Cross and Red Crescent

The Red Cross and Red Crescent Societies are leaders in ensuring the ethical and secure use of data in humanitarian contexts. With sensitive data often collected during disaster responses, the International Federation of Red Cross and Red Crescent Societies (IFRC) and the International Committee of the Red Cross (ICRC) have established robust frameworks to safeguard personal information.

The IFRC's Data Protection Office collaborates with global teams to uphold responsible data management, even in high-pressure situations (International Federation of Red Cross and Red Crescent Societies undated). Their protocols prioritize digital literacy, accountability and transparency, ensuring compliance with international standards. The ICRC's Handbook on Data Protection in Humanitarian Action serves as a cornerstone resource, offering detailed guidance on handling personal data during emergencies (International Committee of the Red Cross 2017). This handbook emphasizes key principles such as data minimization, consent and transparency while addressing emerging technologies like AI and blockchain.

A critical application of these measures is during disaster response operations, where strict protocols ensure that data collected from affected populations – such as geolocation data or health records – is securely stored, anonymized where necessary and never misused. These safeguards demonstrate the importance of balancing urgent humanitarian needs with the rights and privacy of individuals.

The Red Cross's commitment to ethical data use exemplifies how global organizations can responsibly manage sensitive information to support vulnerable communities.

2.5. Harm Mitigation Bodies

In modern societies, harms from data use often extend beyond those who originally provided their data, even without any laws being broken (for more information on harm mitigation in the governance of data use see McMahon, Buyx and Prainsack 2020). For instance, someone might be denied insurance based on predictive analytics, or subjected to relentless targeted advertising due to profiling algorithms exploiting behavioural patterns. Currently, individuals facing these harms often have limited or no avenues for recourse or support.

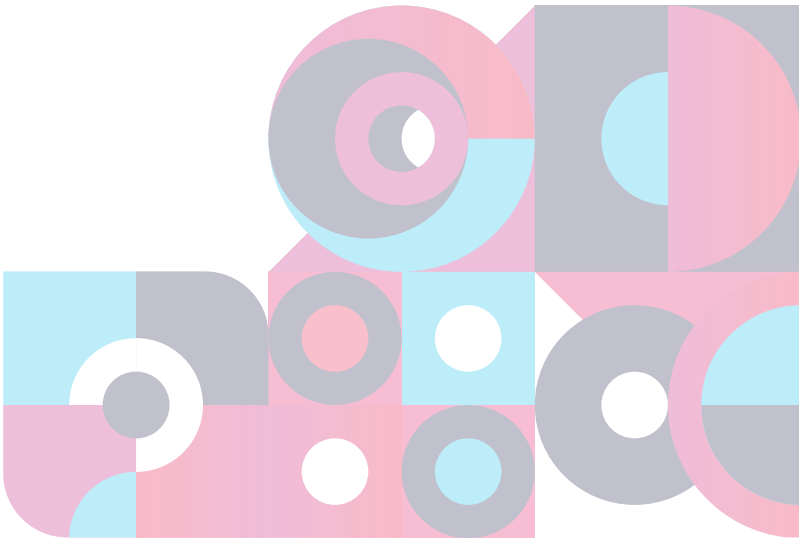
Harm Mitigation Bodies (HMBs) are a proposal emerging from work on data solidarity, which aim to close this gap in traditional legal frameworks by providing financial support and other remedies to those affected by data practices that do not qualify for legal action. They operate on a no-fault basis, meaning people do not need to prove wrongdoing or direct causation to receive assistance. Ideally, algorithms and processes should be designed in a way that minimizes harm from the start. The role of HMBs comes into play if there is a suspicion that harm has occurred nonetheless, often accidentally.

HMBs could be established at a national level, within organizations, or emerge from already-existing data governance structures. See Box 8 for an example scenario.

HMBs have two primary functions:

1. Providing support to individuals harmed by data use
2. Monitoring and reporting on the nature, severity and frequency of such harms

In certain cases, an HMB could provide financial support to assist those harmed. Other forms of support could include e.g. a formal statement of apology on behalf of the relevant organization, or a recommendation from the HMB that the data user take steps to rectify the wrongdoing.



2.5.1. Implementing a Harm Mitigation Body

As HMBs are a novel concept, there is no established path to implement them and they may take many different forms at different levels of governance. The following is a set of recommendations to help you establish an HMB at your own level, be it within a government department, a private organization, or as an independent entity affiliated with larger digital governance structures.

2.5.1.1. Scope and Terms of Reference

Begin by establishing a Terms of Reference to define the HMB's scope, including the types of harms it will address (e.g. financial, emotional, systemic), the supports available and the governance structure.

When defining the types of harms within the HMB's scope, it is important to keep the framework broad, reflecting the diffuse nature of data harms and the HMB's overarching aims. Alberta Virtual Care's harm framework in healthcare, for example, could serve as a model for categorizing data harms (Affleck et al. 2024). Other metrics adapted from health, such as disability-adjusted life years (DALYs), could help quantify data harms and monitor trends (World Health Organization undated).

2.5.1.2. Governance structure

An HMB should have the following as part of its governance structure (see Figure 5):

- **Steering Committee**
  The Steering Committee (SC) governs the HMB, developing decision-making criteria and ensuring procedural transparency. It is staffed by legal and data protection experts, as well as lay members, to ensure diverse perspectives and prevent regulatory capture. The committee oversees the investigative and reporting elements of the HMB and ensures alignment with the HMB's mission.
- **Reporting Branch**
  The Reporting Branch (RB) collects data on harms reported to the HMB, providing insights to improve data governance practices. It collaborates with the Investigative Branch (IB) to identify patterns and inform policy recommendations.
  It plays a crucial role in the HMB's feedback loop to regulators.
- **Investigative Branch**
  The IB handles individual petitions, assessing claims of harm and determining eligibility for support. It works closely with the RB to gather evidence and understand harm patterns, ensures thorough and fair evaluations of claims and feeds information back to the SC.
- **Appeals Panel**
  The Appeals Panel (AP) reviews rejected claims, providing a secondary evaluation to ensure fairness and accuracy and offering an additional layer of oversight. It operates independently but coordinates with the IB to reassess claims.

- **Advisory Board**
  The Advisory Board (AB) oversees the HMB's operations, offering strategic guidance and ensuring alignment with broader data governance goals. Staffed by representatives from data governance bodies, policy experts and public stakeholders, it meets on a regular basis (e.g. annually) to review reports from the SC, IB and RBs and develop standards in conjunction with regional, national or supranational authorities. It ensures the HMB remains responsive to emerging data governance challenges and maintains public trust.

2.5.1.3. Reporting mechanism

The HMB requires a clear mechanism for individuals to report data harm. This could be, for example, a digital platform or hotline, supported by clear guidance on how to use it. The reporting mechanism should allow claims to be submitted as easily and securely as possible and be fully accessible.

2.5.1.4. Financial Support Mechanism

The Financial Support Mechanism of a HMB is designed to provide partial relief to individuals harmed by data use, whether lawful or unlawful. This only applies in cases of hardship and when people have no other source of financial support (e.g. from legal redress systems). Unlike traditional compensation, this support does not aim to fully cover all losses but offers assistance to mitigate the impact of the harm. Applicants can submit informal petitions detailing their harm and its connection to data use.

Financial support would be calculated based on the degree and type of harm suffered by the person. The HMB would assess whether the harm is significant and undue and whether there is a plausible connection between the harm and specific instances of data use.

The amount of financial support offered would aim to reflect the severity of the harm, with more significant harms resulting in higher financial support. Initially, if concerns about affordability arise, financial support could be set as a percentage of losses or costs borne by the individual, such as 60% of the actual loss or costs.

2.5.1.5. Funding

HMBs could be funded through a combination of sources to ensure sustainability and independence. A primary funding source could be a mandatory contribution from data users (e.g. public bodies, companies), set as a percentage of their profits or operational budgets. Additionally, governments could allocate tax revenues to support HMB operations.

Another potential source is a corporate data use tax, where companies benefiting from data use contribute a portion of their earnings. Grants from public and private sectors, as well as international funding bodies, could also supplement the budget. This diversified funding approach ensures robust financial backing for HMB activities.

2.5.1.6. Making a claim to a Harm Mitigation Body

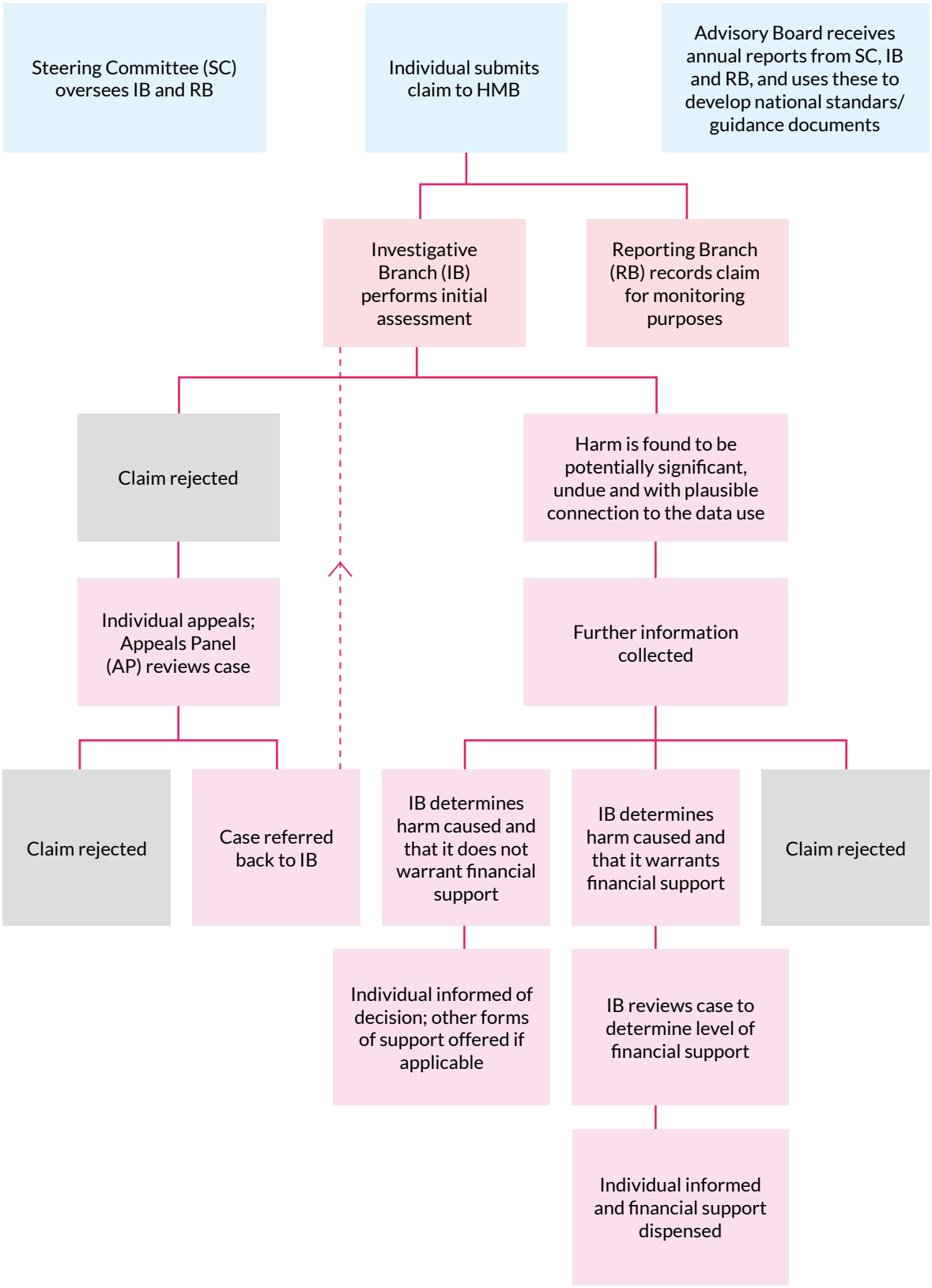
Suppose a person who experiences harm due to data use – such as being denied a loan based on an erroneous algorithmic decision – submits a claim to the HMB. The claim is first recorded by the Reporting Branch (RB) for monitoring purposes, capturing key details like the nature of the harm and the suspected data practices involved. The Investigative Branch (IB) then conducts an initial assessment to evaluate whether the harm is significant, undue and plausibly connected to the data use. For example, they might seek to review the decision-making process behind the algorithm that denied the loan.

If the claim is rejected, the individual can appeal to the Appeals Panel (AP), which either upholds the rejection or refers the case back to the IB for further review. If the harm is deemed potentially significant, the IB may collect additional information, such as documentation of the algorithm's training data, to inform their decision.

Depending on the findings, the IB may reject the claim, approve financial support for the individual (e.g. covering a portion of expenses incurred), or offer other forms of assistance, such as requiring a formal apology, acknowledgement of harm and/or reversal of the decision. The Steering Committee (SC) oversees the IB and RB to ensure fairness, while the Advisory Board (AB) uses annual reports from these branches to, in conjunction with local and national public bodies, refine standards and improve governance practices.

See Box 8 for an example scenario and Figure 5 for a graphical representation of the HMB's decision-making and governance structure.

Figure 5: Proposed decision-making and governance structure for a Harm Mitigation Body (HMB)



Box 8: Harm Mitigation Body at the national level

Marcus, a middle-income professional, notices an unusually high premium on his health insurance renewal. After investigating, he discovers that predictive analytics used by his insurer flagged him as high-risk due to his online activity, such as purchasing certain health supplements. Markus believes this categorization is unfair and decides to file a claim with the newly established National Harm Mitigation Body (HMB).

He submits a form via the HMB's website, outlining his claim and providing evidence of the harm. The HMB's Investigative Branch conducts an initial review and finds that Marcus's case reflects a broader pattern: Several similar complaints have been lodged against insurers using predictive algorithms. The HMB flags this trend to the Ministry with responsibility for data governance, highlighting a systemic risk to public trust.

The HMB's Investigative Branch (IB) collects additional information from Marcus, including financial documentation and evidence of algorithmic profiling. After assessing his case, the IB determines that the harm he experienced was significant, undue and plausibly linked to the data use. While the insurer's actions were legal, the HMB rules that Marcus's harm warrants financial support under its no-fault framework.

The Investigative Branch calculates the degree of harm using predefined criteria, including Markus's financial losses and the psychological impact of being unfairly profiled. Based on this assessment, Marcus receives financial support covering 75% of his increased premium, as well as a formal acknowledgment of the harm he endured.

Beyond supporting Marcus, the HMB uses this case to recommend stricter oversight of predictive analytics in insurance to prevent similar harms, feeding these insights into its annual report to inform policymakers and industry standards.

2.6. Benefit-sharing agreements

Benefit-sharing agreements (BSAs) ensure that profits or other benefits gained from resource use are fairly distributed among the communities or stakeholders that contributed to them. Originally developed in extractive industries such as mining and oil, BSAs are a suggested means to ensure that some of the commercial benefits of data use make their way back to the public sphere. This is important, as it was the public who, by and large, contributed the data in the first place. As such, when private companies benefit from public data, some of those benefits should flow back to the originating individuals and communities.

In practice, a BSA would entail (at a minimum) an agreement between a public body and a data user, in which data is exchanged on the condition that a portion of the benefits emerging from its use makes its way back to the public sphere. This could be in the direct form (i.e. reinvesting profits) or alternatively, by making other benefits (e.g. data insights) freely available.

BSAs could be instituted on a national level, as a statutory element of data sharing when public value is generated. See Box 9 for a hypothetical example of a BSA between a public hospital and a private company.

2.6.1. Functioning of benefit-sharing agreements

BSAs can function through various mechanisms:

1. **Financial compensation:** A portion of the profits from data-driven initiatives is reinvested in public services, infrastructure, or local projects. For example, a private mobility company using city traffic data could contribute a share of its revenue to fund new bike lanes or subsidized public transport in low-income areas
2. **Access to data insights:** Communities receive anonymized data to inform decision-making and research. For instance, a health-tech company using anonymized hospital records for predictive analytics might share insights with public health agencies to improve disease prevention strategies.
3. **Technology sharing:** Public institutions gain access to private-sector technological developments, enhancing service delivery. For example, an AI firm partnering with a public hospital to analyse medical scans could provide the hospital with free or discounted access to its diagnostic tools, improving patient outcomes.

These mechanisms can be implemented at both local and national levels, depending on the scope of the data use and stakeholders involved.

2.6.2. Establishing a benefit-sharing agreement

To implement a BSA at both the local and national levels, policymakers can follow these steps:

1. **Identify and select partners:** Engage public bodies and private entities willing to collaborate on a BSA, ensuring alignment with community priorities.
2. **Public consultation:** Gather input from affected communities to define expected benefits and address potential concerns.
3. **Draft and negotiate the BSA:** Develop an agreement with legal counsel outlining the structure, governance and terms, including how benefits will be distributed.
4. **Implementation and monitoring:** Enforce the agreement while maintaining regular oversight and transparency.
5. **Evaluation and reporting:** Assess outcomes, publish findings and explore broader applications of the BSA model.

2.6.2.1. Governance structure

A BSA should have a clear governance structure to ensure transparency, accountability and equitable distribution of benefits. At a minimum, this should include:

- **Supervisory Panel**
  Oversees the implementation of the BSA, ensuring compliance with agreed terms and facilitating communication between public institutions, private partners and affected communities. For example, a local hospital's board and representatives from the partnering tech company could jointly oversee the reinvestment of profits into community health programmes.
- **Public Oversight Mechanism**
  Engages community representatives, independent watchdogs, or civil society organizations to monitor the BSA's impact and ensure that agreed benefits are delivered. For instance, a citizen advisory board could regularly review reports on how funds generated from data use are reinvested in public health initiatives.
- **Independent Evaluation Body**
  Conducts periodic assessments of the BSA's effectiveness, ensuring that financial contributions, data access, or technology sharing align with the original objectives. An independent audit might verify that a company using anonymized patient data for drug development has fulfilled its obligation to provide discounted medicines to local clinics, for instance.

  By embedding these governance mechanisms, policymakers can ensure that BSAs remain accountable, effective and aligned with community needs.

  See Box 9 for an example of a hypothetical BSA between a local hospital and technology firm.

Box 9: A benefit-sharing agreement (BSA) between a public hospital and a private health tech company

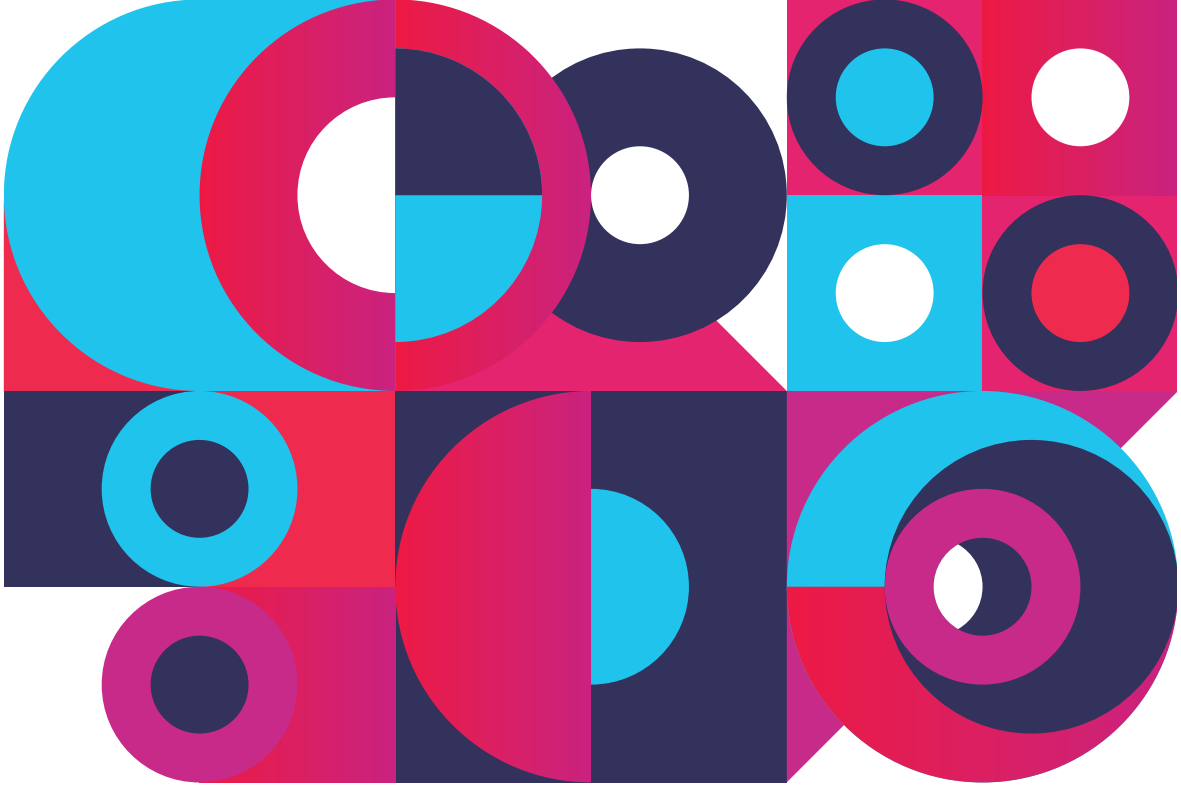
The research hospital Maastricht University Medical Center (UMC) decides to enter into a partnership with a private health technology company, MediTech Analytics, that develops predictive analytics for disease prevention. Under the agreement, Maastricht UMC provides anonymized patient data, including demographics, medical histories and treatment outcomes, which MediTech Analytics uses to enhance its AI-driven diagnostic tools. In exchange, the company commits to reinvest a portion of the profits derived from the data use into public health initiatives in Maastricht while also granting the hospital access to its refined predictive models at no cost.

The agreement is structured through a formal Memorandum of Understanding (MoU), outlining clear terms on data use, governance and benefit distribution. Public consultations ensure community concerns – such as privacy safeguards and fair distribution of reinvested funds – are addressed before implementation. A Steering Committee, comprising hospital administrators, company representatives and local health advocates, oversees compliance and monitors progress.

The BSA is drafted and signed with the following conditions:

- **Financial reinvestment:** MediTech Analytics allocates 10% of profits generated from commercial licensing of the AI model towards expanding healthcare services in the hospital's catchment area. This funds new mobile clinics and subsidized treatment for low-income patients
- **Access to data insights:** Maastricht UMC receives real-time analytics on disease trends and patient risk factors, helping medical staff tailor preventive care strategies.
- **Technology sharing:** The company integrates its AI diagnostics into the hospital's systems free of charge, enhancing early detection of chronic illnesses.

After two years, independent evaluations confirm improved healthcare outcomes, with a 15% reduction in preventable hospital admissions. Community representatives on the Public Oversight Board ensure reinvested funds reach underserved areas, reinforcing trust and accountability.



3. Resources

The list below are recommened resources to engage further with the concepts of data solidarity and public value, particularly in the context of health.

- PLUTO (El-Sayed et al. 2023)
- White Paper: data solidarity (Prainsack et al. 2025)
- Data Solidarity Glossary (Prainsack and Kickbusch 2024).
- Data solidarity: a blueprint for governing health futures (Prainsack et al. 2022)
- The *Lancet* and *Financial Times* Commission on governing health futures 2030: growing up in a digital world (Kickbusch et al. 2021)
- Big Data governance needs more collective responsibility: the role of harm mitigation in the governance of data use in medicine and beyond (McMahon, Buyx and Prainsack 2020)
- Solidarity in biomedicine and beyond (Prainsack and Buyx 2017)

References

Affleck, E., Tam, S., Bucci, S., Lindeman, C., Hunter, R., Mita, R., McPhail, B., Spithoff, S., Murphy, T., Krempien, J., Kitchen, A., MacQueen, A., Millar, C., Sham, C., Krecsy, S., Fraser, S., Joshi, R, Schamper, A. and Lucyk, A. (2024). *Data disarray: A root cause analysis of health data dysfunction in Canada*. Alberta Virtual Care Coordinating Body. https://www.networked-health.org/_files/ugd/3eb345_85ada6635d334c2ba6c102bdd57f20e2.pdf (Accessed July 29, 2025).

Agbo, M. Jr. (2023, August 23). *The problem with solid waste management in Nigeria's low-income neighbourhoods*. Earth.org. https://earth.org/the-problem-with-solid-waste-management-in-nigerias-low-income-neighbourhoods/ (Accessed July 22, 2025).

Akter, S., Dwivedi, Y.K., Sajib, S., Biswas, K., Bandara, R.J. and Michael, K. (2022). Algorithmic bias in machine learning-based marketing models. *Journal of Business Research*, *144*, 201-216. https://doi.org/10.1016/j.jbusres.2022.01.083

Allam, Z. and Jones, D.S. (2020). On the coronavirus (COVID-19) outbreak and the smart city network: Universal data sharing standards coupled with artificial intelligence (AI) to benefit urban health monitoring and management. *Healthcare*, *8*(1), Article 46. https://doi.org/10.3390/healthcare8010046

Almukhalfi, H., Noor, A. and Noor, T.H. (2024). Traffic management approaches using machine learning and deep learning techniques: A survey. *Engineering Applications of Artificial Intelligence*, *133*(Part B), Article 108147. https://doi.org/10.1016/j.engappai.2024.108147

Autoriteit Persoonsgegevens. (2020). *Belastingdienst/Toeslagen. De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag* [Tax and Customs Administration/Benefits: Processing the nationality of applicants for childcare allowance]. https://www.autoriteitpersoonsgegevens.nl/uploads/imported/onderzoek_belastingdienst_kinderopvangtoeslag.pdf (Accessed 29 July, 2025).

Baker, M. (2021, October 1). *Everything you need to know about the MyFitnessPal data breach*. UK Tech News. https://uktechnews.co.uk/2021/10/01/everything-you-need-to-know-about-the-myfitnesspal-data-breach/ (Accessed July 22, 2025).

BBC. (2019, July 11). *France passes tax on tech giants despite US threats*. https://www.bbc.co.uk/news/world-europe-48947922 (Accessed July 22, 2025).

BBC. (2022, February 2). *Mental health helpline ends data-sharing relationship*. https://www.bbc.com/news/technology-60218894 (Accessed July 22, 2025).

Big Brother Watch. (2024, May 24). *Landmark legal challenges launched against facial recognition after police and retailer misidentifications* [Press release]. https://bigbrotherwatch.org.uk/press-releases/landmark-legal-challenges-launched-against-facial-recognition-after-police-and-retailer-misidentifications/https://bigbrotherwatch.org.uk/press-releases/landmark-legal-challenges-launched-against-facial-recognition-after-police-and-retailer-misidentifications/ (Accessed July 22, 2025).

Birhane, A. (2022). The unseen Black faces of AI algorithms. *Nature, 610*(7932), 451-452. https://doi.org/10.1038/d41586-022-03050-7

Block, V. (2024, October 28). City government looks to AI to improve services. *Crain's New York Business*. https://www.crainsnewyork.com/technology/new-york-city-government-looks-ai-improve-services (Accessed July 23, 2025).

Charnock, G., March, H. and Ribera-Fumaz, R. (2021). From smart to rebel city? Worlding, provincialising and the Barcelona Model. *Urban Studies*, *58*(3), 581-600. https://doi.org/10.1177/0042098019872119;

Chen, Z. (2023). Ethics and discrimination in artificial intelligence-enabled recruitment practices. *Humanities and Social Sciences Communications*, *10*, Article 567. https://doi.org/10.1057/s41599-023-02079-x

Donaldson, D.R. and Koepke, J.W. (2022). A focus groups study on data sharing and research data management. *Scientific Data*, *9*, Article 345. https://doi.org/10.1038/s41597-022-01428-w

El-Sayed, S., Prainsack, B., Hogan, C., Möller, T., Ferenc Gyarmati, P., Jordan, B., Koesten, L. and Forgó, N. (2023). *PLUTO – Public Value Assessment Tool*. University of Vienna. https://pluto.univie.ac.at/ (Accessed July 23, 2025).

Fahey, D. (2021, January 20). *The app that helps you shop ethically – and what I learned using it.* Positive News. https://www.positive.news/economics/the-app-that-helps-you-shop-ethically-and-what-i-learned-using-it/ (Accessed July 23, 2025).

Goodstack. (undated). *The Purpose Blog*. https://goodstack.io/blog (Accessed July 29, 2025).

Government of Canada. (2023). *The Artificial Intelligence and Data Act (AIDA) – companion document*. https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document (Accessed July 23, 2025).

Greenhow, C., Lewin, C. and Staudt Willet, K.B. (2021). The educational response to Covid-19 across two countries: A critical examination of initial digital pedagogy adoption. *Technology, Pedagogy and Education*, *30*(1), 7-25. https://doi.org/10.1080/1475939X.2020.1866654

Huber, N. (2022, June 1). Transport systems give hackers a moving target. *Financial Times*. https://www.ft.com/content/dc3cccb0-533c-4c5b-bc20-5ee3d422909f (Accessed July 23, 2025).

Hutchinson, A., 2021, July 5. *Norway introduces new law forcing disclosure on retouched photos posted online*. Social Media Today. https://www.socialmediatoday.com/news/norway-introduces-new-law-forcing-disclosure-on-retouched-photos-posted-onl/602832/ (Accessed July 23, 2025).

International Committee of the Red Cross (ICRC). (2017, June 28). *About the handbook*: https://www.icrc.org/en/document/data-protection-handbook (Accessed July 23, 2025).

International Federation of Red Cross and Red Crescent Societies (IFRC). (undated). *Data protection*. https://www.ifrc.org/our-promise/do-good/data-protection (Accessed July 23, 2025).

Jacobs, K. (2022, June 29*). Toronto wants to kill the smart city forever.* MIT Technology Review. https://www.technologyreview.com/2022/06/29/1054005/toronto-kill-the-smart-city/ (Accessed August 25, 2025).

Jones, C., McDowell, A., Galvin, V. and Adams, D. (2022). Building on Aotearoa New Zealand's integrated data infrastructure. *Harvard Data Science Review*, *4*(2). https://doi.org/10.1162/99608f92.d203ae45

Kickbusch, I., Piselli, D., Agrawal, A., Balicer, R., Banner, O., Adelhardt, M., Capobianco, E., Fabian, C., Gill, A.S., Lupton, D., Medhora, R.P., Ndili, N., Ryś, A., Sambuli, N., Settle, D., Swaminathan, S., Vega Morales, J., Wolpert, M., Wyckoff, A.W. and Xue, L. on behalf of the Secretariat of the Lancet and Financial Times Commission. (2021). The *Lancet* and *Financial Times* Commission on governing health futures 2030: Growing up in a digital world. *The Lancet*, *398*(10312), 1727-1776. https://doi.org/10.1016/S0140-6736(21)01824-9

Lagos Waste Management Authority (LAWMA). (2021). *Lagos Waste Management Authority* (Version 14.0) [Mobile app]. https://lawma.gov.ng/apps/ (Accessed July 23, 2025).

Leisinger, K.M., Garabedian, L.F. and Wagner, A.K. (2012). Improving access to medicines in low and middle income countries: Corporate responsibilities in context. *Southern Med Review*, *5*(2), 3-8. https://pmc.ncbi.nlm.nih.gov/articles/PMC3606933/

Lu, D. (2020, June 19). Uber and Lyft pricing algorithms charge more in non-white areas. *New Scientist*. https://www.newscientist.com/article/2246202-uber-and-lyft-pricing-algorithms-charge-more-in-non-white-areas/ (Accessed July 23, 2025).

McMahon, A., Buyx, A. and Prainsack, B. (2020). Big data governance needs more collective responsibility: The role of harm mitigation in the governance of data use in medicine and beyond. *Medical Law Review*, *28*(1), 155-182. https://doi.org/10.1093/medlaw/fwz016

Monge, F., Barns, S., Kattel, R. and Bria, F. (2022). *A new data deal: The case of Barcelona* (IIPP Working Paper 2022/02). UCL Institute for Innovation and Public Purpose. https://www.ucl.ac.uk/bartlett/public-purpose/wp2022-02 (Accessed July 23, 2025).

National Health Authority (NHA). (2023). *Ayushman Bharat Digital Mission*. https://abdm.gov.in (Accessed July 29, 2025).

Neuroni, A.C., Haller, S., van Winden, W., Carabias-Hütter, V. and Yildirim, O. (2019). Public value creation in a smart city context: An analysis framework. In M.P. Rodríguez Bolívar (Ed.), *Setting foundations for the creation of public value in smart cities* (pp. 49-76). Springer. https://doi.org/10.1007/978-3-319-98953-2_3

Pandey, A. and Caliskan, A. (2020). Disparate impact of artificial intelligence bias in ridehailing economy's price discrimination algorithms. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society (AIES '21)*, pp. 822-833. Association for Computing Machinery. https://doi.org/10.1145/3461702.3462561

Porter, J. (2019, July 22). *Equifax agrees to settlement of up to $700 million over 2017 data breach*. The Verge. https://www.theverge.com/2019/7/22/20703497/equifax-ftc-fine-settlement-2017-data-breach-compensation-fund (Accessed July 23, 2025).

Powles, J. and Hodson, H. (2017). Google DeepMind and healthcare in an age of algorithms. *Health and Technology*, *7*(4), 351-367. https://doi-org.uaccess.univie.ac.at/10.1007/s12553-017-0179-1

Prainsack, B. (2017). Research for personalised medicine: Time for solidarity. *Medicine and Law*, *36*(1), 87-98. https://heinonline.org/HOL/LandingPage?handle=hein.journals/mlv36&div=10&id=&page=

Prainsack, B., El-Sayed. S., Forgó, N., Szoszkiewicz, Ł. and Baumer, P. (2022). Data solidarity: A blueprint for governing health futures. *The Lancet Digital Health*, *4*(11), e773 - e774. https://doi.org/10.1016/S2589-7500(22)00189-3

Prainsack, B., El-Sayed, S., Forgó, N., Szoszkiewicz, Ł. and Baumer, P. (2025). *Data solidarity – a White Paper.* Geneva: Governing Health Futures 2030. https://dthlab.org/wp-content/uploads/2025/02/25_01-DTH-Lab-Data-Solidarity-White-Paper.pdf (Accessed August 12, 2025).

Prainsack, B. and Buyx, A. (2017). *Solidarity in biomedicine and beyond.* Cambridge University Press. https://doi.org/10.1017/9781139696593

Prainsack, B. and Kickbusch, I. (2024). *Data Solidarity Glossary*. Geneva: Digital Transformations for Health Lab. https://dthlab.org/wp-content/uploads/2024/09/DTH-Data-Solidarity-Glossary-2024.pdf (Accessed August 12, 2025).

Rush, K.L., Singh, S., Seaton, C.L., Burton, L., Li, E., Jones, C., Davis, J.C., Hasan, K., Kern, B. and Janke, R. (2022). Telehealth use for enhancing the health of rural older adults: A systematic mixed studies review. *The Gerontologist*, *62*(10), e564-e577. https://doi.org/10.1093/geront/gnab141

Sharma, R.S., Rohatgi, A., Jain, S. and Singh, D. (2023). The Ayushman Bharat Digital Mission (ABDM): Making of India's digital health story. *CSI Transactions on ICT*, *11*(1), 3-9. https://doi.org/10.1007/s40012-023-00375-0

Statistics New Zealand. (2022, August 23). *Integrated Data Infrastructure (IDI)*. https://www.stats.govt.nz/integrated-data-infrastructure/ (Accessed July 23, 2025).

Strava Support. (2024, August 1). *Strava Metro and the Global Heatmap*. Available at: https://support.strava.com/hc/en-us/articles/216918877-Strava-Metro-and-the-Global-Heatmap (Accessed July 23, 2025).

Strielkowski, W., Zenchenko, S., Tarasova, A. and Radyukova, Y. (2022). Management of smart and sustainable cities in the post-COVID-19 era: Lessons and implications. *Sustainability*, *14*(12), Article 7267. https://doi.org/10.3390/su14127267

ten Seldam, B. and Brenninkmeijer, A. (2021, April 30). The Dutch benefits scandal: A cautionary tale for algorithmic enforcement. *EU Law Enforcement*. https://eulawenforcement.com/?p=7941 (Accessed July 23, 2025).

The Jerusalem Post (2024, February 18). AI falsely accuses, fines artificial intelligence expert of using phone while driving – report. https://www.jpost.com/business-and-innovation/tech-and-start-ups/article-787534 (Accessed July 23, 2025).

The Straits Times (2018, July 20). SingHealth cyber attack: How it unfolded. https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html (Accessed July 23, 2025).

Wakefield, J. (2019, May 18). The Google city that has angered Toronto. *BBC*. https://www.bbc.com/news/technology-47815344 (Accessed August 25, 2025).

Weakley, K. (2023, October 25). *Frustration as funding for deprived communities shifted to small towns*. Local Government Chronicle (LGC). https://www.lgcplus.com/services/regeneration-and-planning/frustration-as-funding-for-deprived-communities-shifted-to-small-towns-25-10-2023/ (Accessed July 23, 2025).

World Health Organization (WHO). (undated). *Disability-Adjusted Life Years (per 100,000 population)*. https://www.who.int/data/gho/indicator-metadata-registry/imr-details/156 (Accessed July 29, 2025).

Digital Transformations for Health Lab (DTH-Lab)
Hosted by: The University of Geneva
Campus Biotech, Chemin des Mines 9
1202 Geneva, Switzerland
Email: team@dthlab.org

www.DTHLab.org