Trustworthy Data Institutional Framework

A practical tool to improve trustworthiness in data ecosystems

October 2023

GPAI | THE GLOBAL PARTNERSHIP ON ARTIFICIAL INTELLIGENCE

This report was developed by Experts and Specialists involved in the Global Partnership on Artificial Intelligence's project on Data Institutions. The report reflects the personal opinions of the GPAI Experts and External Experts involved and does not necessarily reflect the views of the Experts' organisations, GPAI, or GPAI Members. GPAI is a separate entity from the OECD and accordingly, the opinions expressed and arguments employed therein do not reflect the views of the OECD or its Members.

Acknowledgements

This report was developed in the context of the Data Institutions Project, with the steering of the Project Co-Leads and the guidance of the Project Advisory Group, supported by the GPAI Data Governance Working Group. The GPAI Data Governance Working Group agreed to declassify this report and make it publicly available.

Co-Leads:

- **Teki Akuetteh Falconer***, Africa Digital Rights Hub

The report was written by:

- **Thomas Hervé Mboa Nkoudou**, CEIMIA
- **Stephanie King,** CEIMIA

GPAI recognizes the dedication of contributors of local organizations who played a pivotal role through the whole project: **Fomekong Félicien**‡, National Institute of Statistics (Cameroon); **Ngie Pierre Joel,** Minrex (Cameroon); **Bekono Nkoudou Hugues,** Minrex (Cameroon), **Aristide Donald BILOUNGA**‡, IPREVA (Cameroon); **Jafsia Élisée**‡, SDI, (Cameroon); **Kengne Tagne Yannick Ghislain**‡, AIDER (Cameroon); **MAHAMAT Allamine**‡, CADEPI (Cameroon).

GPAI would like to thank **Laurie Parenteau**‡ of Créations Laurie, for her diligent and efficient work in bringing the visual components of this work to life. GPAI also recognizes the meaningful contribution of ODI/Microsoft Peer Learning Network trainees who shared their feedback on the co-design of the framework.

GPAI would like to acknowledge the tireless efforts of colleagues at the International Centre of Expertise in Montréal on Artificial Intelligence (CEIMIA) and GPAI's Data Governance Working Group. We are grateful, in particular, for the support **Sophie Fallaha, Mathieu Marcotte, Stephanie King**, **Gwenaelle Le Peuch, Noemie Gervais, Arnaud Quenneville-Langis, Janick Houde,** and **Caroline Renaud** from CEIMIA, and for the dedication of the Working Group Co-Chairs **Jeni Tennison*** and **Maja Bogataj Jančič*.**

* Expert
** Observer
† Invited Specialist
‡ Contracted Parties by the CofEs to contribute to projects

Citation

GPAI 2023. Trustworthy Data Institutional Framework: A practical tool to improve trustworthiness in data ecosystems, Report, October 2023, Global Partnership on AI.

Table of Contents

Preface **2**
Executive Summary **3**
Introduction **4**
Trustworthiness in the data lifecycle **4**
Element 1: The extended data lifecycle 5
Element 2: The combined data governance approach 6
Element 3: Interchangeability of the data stewardship role 8
Element 4: Mechanisms for interaction 10
Trustworthiness Assessment **12**
A Commons-based approach to trustworthiness 12
Trustworthiness indicators and their variables 12
The TDI-Maturity Tool 17
Conclusion **21**
Bibliography **22**
Appendix A: Description of variables by levels of maturity **23**
SHARED RESOURCES 23
COMMUNITIES 26
RULES 27
GOVERNANCE 30
Appendix B: Actions to take to improve trustworthiness **33**
FROM UNAWARE TO EMERGING 33
FROM EMERGING TO LEARNING 33
FROM LEARNING TO DEVELOPING 33
FROM DEVELOPING TO MASTERING 33
Appendix C: Glossary **34**
Appendix D: Printable Version of the Evaluation Grid **36**

Preface

The Global Partnership on Artificial Intelligence (GPAI) is a multi-stakeholder initiative which aims to bridge the gap between theory and practice on AI by supporting cutting-edge research and applied activities on AI-related priorities[1]. GPAI brings together 29 Members and approximately 130 leading AI experts to advance the responsible use, development and deployment of AI towards shared global challenges. GPAI Experts collaborate across four Working Groups on the themes of responsible AI, data governance, the future of work, and innovation and commercialization.

The Data Governance Working Group provides expertise to promote data for AI being collected, used, shared, archived and deleted in ways that are consistent with human rights, inclusion, diversity, innovation, economic growth, and societal benefit, while seeking to address the UN Sustainable Development Goals. In line with this approach, GPAI worked with the ODI and Aapti Institute to explore real-world use cases and operationalisation strategies where data trusts could offer social benefits to the community(GPAI, 2021b). When conducting a feasibility assessment, the ODI & Aapti team found a potential in data trusts to enable communities to use data to advocate for, and inform the design of, sustainable infrastructure. Although, the team indicated some challenges for the broader implementation of data trusts in the Global South. The GPAI's Data Governance (DG) Working Group then recommended considering wider, bottom-up data institutions and trustworthy practices where communities are empowered around their data, without the need for trustees with fiduciary obligation (GPAI, 2021a, 2022d).

To carry forward this recommendation, CEIMIA researchers identified climate-induced migration in Lake Chad Basin[2] as a use case, conducting fieldwork in Cameroon to scan the local data ecosystem in order to understand: Who are the key stakeholders? What are the dynamics between data institutions and affected communities? What are the gaps and challenges data governance faces in such a context? This investigation led to two key findings: there exists some gaps and challenges (for example: availability of climate migration data, uncertainties on the sustainability of data collection activities, lack of access to existing data, etc..) preventing the true participation of local organisations and affected communities in the data governance process, and, there is a lack of trust amongst key stakeholders of the data ecosystem (GPAI, 2023). However, these challenges are not insurmountable based on both the solutions heard from local stakeholders and scientific works already done by GPAI Experts.

As part of the DG Working Group's work, this exercise sought to provide an answer to the above gaps, through the co-design of a framework allowing data institutions to develop the safe, fair, and equitable sharing of data while empowering individuals and communities to assert their data rights. Hence the Trustworthy Data Institutional Framework (TDIF) which is, on one hand, a description of capacities and values needed by any organisation stewarding data in order to build trust; and on the other hand, the assessment of trustworthiness maturity in data practices.

Sophie Fallaha
Directrice générale | Executive Director

[1] https://gpai.ai/about/

[2] A region covering Nigeria, Niger, Chad and Cameroon; and grappling with a complex humanitarian crisis with over 3.2 million people displaced due to floods, scarce water supplies, degraded farmlands, food insecurity, and farmers-herders conflicts.

Executive Summary

In 2020, GPAI commissioned the Open Data Institute and Aapti Institute to explore real-world use cases and operationalisation strategies where data trusts could offer societal benefit with a focus on AI and climate action. From this foundational work by the ODI and Aapti teams, emerged some limitations[3]. That is why, the Data Governance Working Group recommended considering wider, bottom-up data institutions and trustworthy practices where communities are empowered around their data. For this purpose, we conducted a pilot study in Cameroon, where we mapped the data ecosystem by identifying the different stakeholders, described the dynamics in data collection, identified gaps and challenges and presented some concrete actions to mitigate these challenges. Taken into account by data institutions, these actions provide a path to improve trustworthiness in data governance. But this is only possible within an integrated data governance system that places the values of sharing and openness at the center of data exchange. Hence the Trustworthy Data Institutional Framework that we co-designed with local organisations during the ODI/Microsoft Peer Learning Network Programme.

The Trustworthy[4] Data Institutional Framework (TDIF) is a practical tool enabling organisations that manage data to understand where they currently stand with regards to their data governance, while providing a path to improve trustworthiness (ODI, 2021). The TDIF consists of two parts:

- The first part, representing the ideal vision of trustworthiness in data institutions that enables the development of safe, fair, and equitable sharing of data while empowering individuals and communities to assert their data rights. This vision is built on four key aspects: (1) the extended data lifecycle, (2) the combined data governance approach, (3) the interchangeability of the data stewardship role, and (4) the dynamics of engagement and responsibilities.
- The second part, representing the trustworthiness assessment tool we have designed, which allows organisations to assess where they stand in terms of trust in their data practices.The assessment tool incorporates maturity levels, an evaluation grid, and a scoring methodology. Once an organisation knows its level of maturity, it can then take some concrete actions suggested in the annex, to improve its level of trustworthiness.

The first organisations to test the TDIF recognise its importance and see its application in different sectors. However, a need has emerged to see this tool automated with an online version. Automating the TDIF is therefore the next step in this project.

[3] GPAI 2022. Enabling Data Sharing for Social Benefit Through Data Trusts: Data Trusts in Climate, Report, March 2022, Global Partnership on AI

[4] We use 'trustworthy' to mean an organisation is worthy of being trusted, while 'trust' refers to an organisation actually being trusted by an individual, organisation or ecosystem. An organisation can be trustworthy without being trusted (and trusted without being trustworthy).
https://open-data-institute.gitbook.io/p22-trustworthy-data-stewardship-guidebook/-MW92wuAXMrYPE7sgA-M/introduction/overview

Introduction

Nowadays, data is an important part of our society, and proper data governance has become crucial to fully benefit from technologies based on artificial intelligence. However, many challenges hinder data governance and spoliate individuals and communities to their rights over the data they generate in their day to day lives. Regardless of the organisation, the context, or the communities involved, these challenges are exacerbated with the rise of AI and related fields. This brings a main question to the table of many organisations: what strategic and comprehensive approach to data governance needs to be put in place to better enforce data rights and/or digital rights? In other words, what is the best way to improve how data is being collected, stewarded, shared, and used, to better serve the needs of communities and empower them to play an active role in the data value chain?

On the basis of its previous work, the GPAI's Data Governance Working Group has identified data institutions (with a wider lens than data trusts[5]) as one of the ways that can be beneficial in helping minimise the challenges facing data governance and the enforcement of data rights or digital rights[6], leading to the recommendation to consider existing data institutions and document existing forms of trustworthy practices (GPAI, 2021b). As part of the ongoing work carried out by the Data Governance working group and the desire to put the above recommendation into practice, we are pleased to present in this report, the **Trustworthy[7] Data Institutional Framework (TDIF);** which is a practical tool enabling organisations that manage data to understand where they currently stand with regards to their data governance, while providing a path to improve trustworthiness (ODI, 2021).

Trustworthiness in the data lifecycle

The GPAI Data Governance Working Group's Data Governance Framework 2.0[8] serves as the baseline document for this report, giving an overview of the most relevant terms and defining the collective understanding of the Working Group (GPAI, 2022c). Moreover, the document highlights three primary aspects of data governance which can help to define trustworthiness in this context:

- The governance of AI training and testing data, which involves a functional perspective, in which what counts is that the resulting solutions are trustworthy and responsible;
- The governance of algorithmic input and output data, which includes individual and collective rights addressed by data privacy/protection law or other bodies of the law such as the indigenous knowledge rights and protections;
- The governance of wider data ecosystems, which includes the quest of data justice.

The approach of trustworthiness adopted in the TDIF relates most closely to this final aspect. While this type of governance looks at the location and means of data storage, as well as the way data is accessed and shared, it may also consider bigger societal, economic and environmental effects (GPAI, 2022c, p. 15).

In the data lifecycle, to achieve this ideal state of trustworthiness that enables the development of safe, fair, and equitable sharing of data while empowering individuals and communities to assert their data rights, data institutions should consider the following elements: (1) the extended data

[5] Data trusts are a new form of data stewardship; they are a type of data institution that supports individuals or groups to pool resources, tasking an independent 'trustee' to manage those resources for the benefit of the trust's members (page 4).

[6] The Aapti Institute's review of global legal frameworks also highlights a diversity of policy approaches towards data stewardship across the globe. Countries differ in: the extent to which their current legislation provides data rights for individuals or communities, the ways in which those rights – where they exist – can be enacted through data institutions (page 6).

[7] We use 'trustworthy' to mean an organisation is worthy of being trusted, while 'trust' refers to an organisation actually being trusted by an individual, organisation or ecosystem. An organisation can be trustworthy without being trusted (and trusted without being trustworthy). https://open-data-institute.gitbook.io/p22-trustworthy-data-stewardship-guidebook/-MW92wuAXMrYPE7sgA-M/introduction/overview

[8] Data Governance Working Group: A Framework Paper for GPAI's Work on Data Governance 2.0

lifecycle, (2) the combined data governance approach, (3) the interchangeability of the data stewardship role, and (4) the dynamics of engagement and responsibilities.

Element 1: The extended data lifecycle

The Data Governance Framework provides us with the simplified data-centred data lifecycle (see the picture below) which includes steps such as the creation, collection, preparation, use, retention or preservation, sharing, re-use or deletion of data (GPAI, 2022c, p. 11).

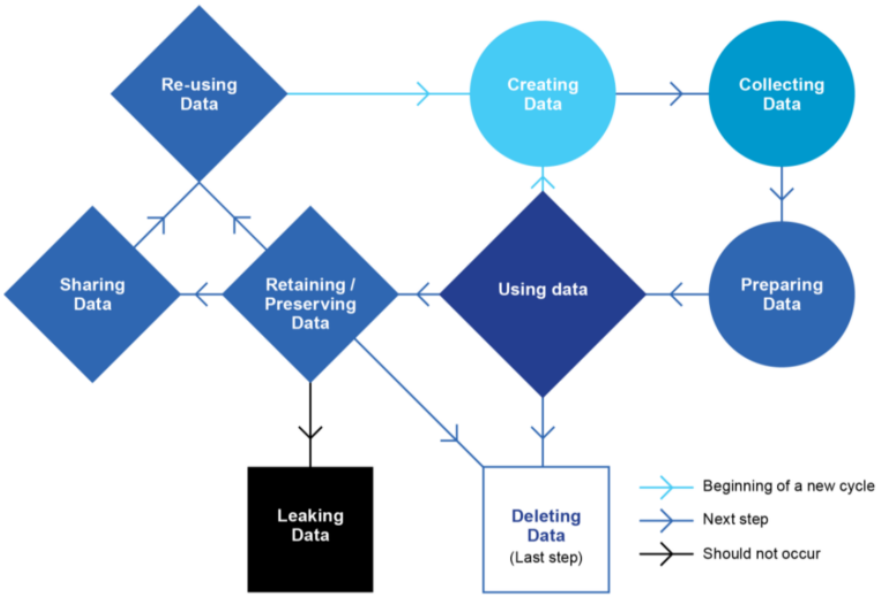


***Figure 1** : The simplified data-centred data lifecycle* (source: Data Governance Framework 2.0., P11)

However, during the fieldwork in Cameroon[9], gaps and challenges were identified in data governance. Firstly, barriers to participation of local communities in data governance due to restricted access to data collected, lack of data literacy, etc. Secondly, there exists a lack of relevant data due to financial limitations of local organisations, and a lack of suitable infrastructures to capture various relevant data. These challenges highlight the importance of also considering the following aspects, when thinking about the data lifecycle:

- Data Literacy and Capacity Building for local communities/organisations; and
- Inclusive Data Infrastructure and Tools to ensure a fair and equitable participation of all data ecosystem stakeholders (including local communities/organisations).

By adding these two points to the simplified data-centred data lifecycle suggested by the Data Governance Framework 2.0, the report presents the extended data lifecycle:

[9] Designing Trustworthy Data Institutions Scanning the Local Data Ecosystem in Climate-Induced Migration in Lake Chad Basin - Pilot Study in Cameroon

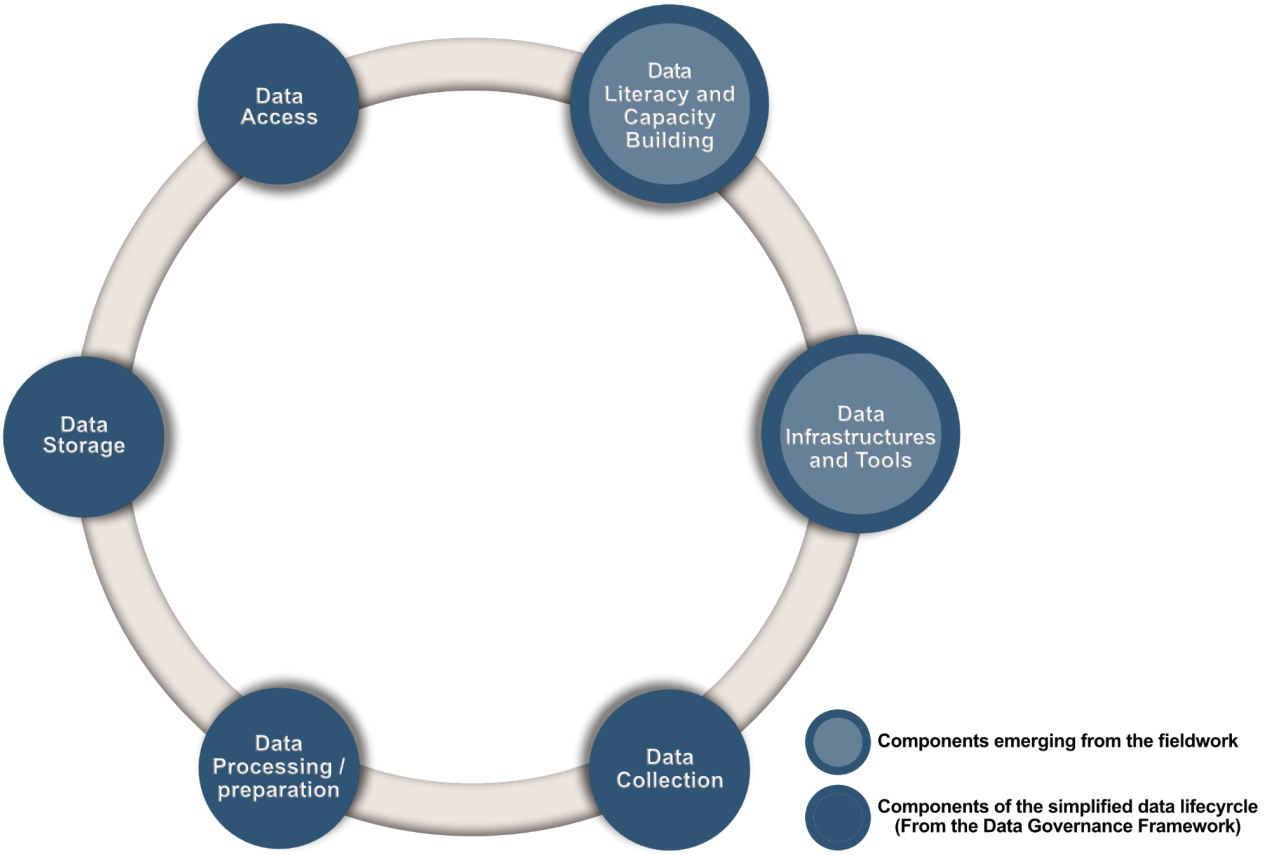


***Figure 2**: The extended data lifecycle*

***NB:** For the purpose of this work, we will use "Data Access" as an umbrella term to cover aspects related to creation, use; while retention or preservation fit under "data storage", sharing, re-use or deletion of data. However, it should be noted that the various stages of the extended data lifecycle are not isolated, but are instead interconnected by a governance system as described below.*

Element 2: The combined data governance approach

The combined data governance approach is built from the recommendation in the Data Governance Framework 2.0, which advises to focus on data governance, and consider the multistakeholder approach as well as the principled approach.

The multistakeholder approach of data governance requires consideration of policymakers, data holders, individuals and communities; as well as it defines whose task (sectoral, cross-sectoral) at what level (national, supranational or international) (GPAI, 2022c, pp. 16–17). The ethical and principled approach of data governance consider:

- policies that should guide any decision to be made about data throughout the data lifecycle;
- requirements to be met by any concrete data activities; and
- standards for data preparation and storage to create sustainable value and data sharing.

The Data Governance Working Group has systematised these principles as follows (GPAI, 2022c, pp. 18–19):

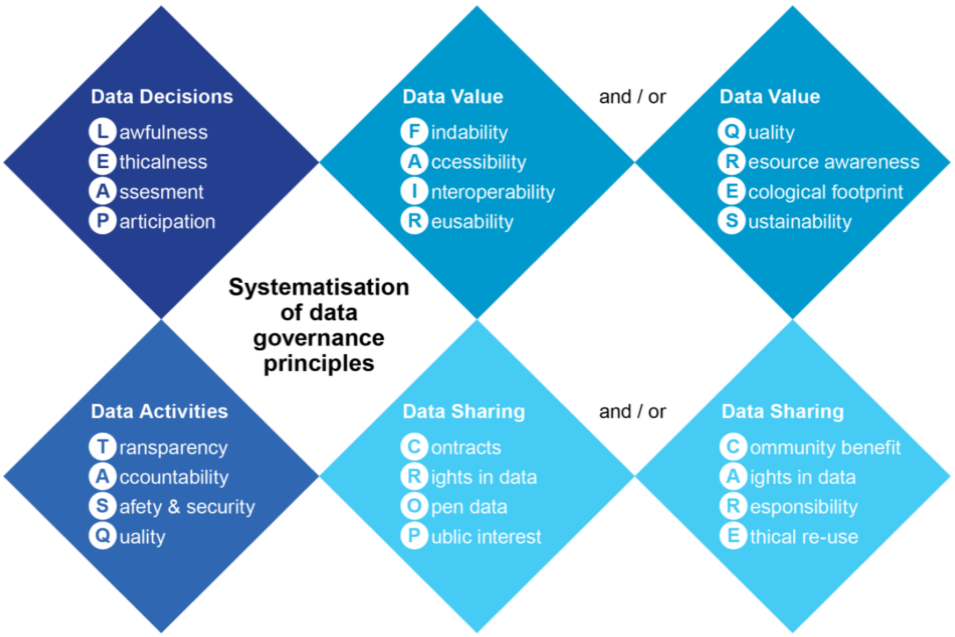


***Figure 3**: Systematisation of data governance principles* (source: Data Governance Framework 2.0, p19)

- **Data Decisions** (LEAP): LEAP - Relevant governance decisions must be lawful and ethical, they must be subject to careful assessment (including wider impacts) and seek participation of all relevant stakeholders;
- **Data Activities** (TASQ): TASQ - There is a consensus that transparency, accountability, safety and security as well as a high level of data quality in the sense of the data being appropriate to the task;
- **Data Value** (FAIR/QRES)**:** FAIR - Known as findability, accessibility, interoperability and reusability, is really useful when it comes to creating data value and enhancing access to as well as sharing and re-use of data; and/or QRES - An attitude that stresses quality, resource and wider ecological footprint awareness as well as sustainability.
- **Data Sharing** (CROP/CARE)**:** CROP - stress the existence of, and the need to enhance, different cross-sectoral frameworks for data sharing and corresponding access and control mechanisms such as contractual agreements, portability and similar rights in data, open data and more restricted arrangements, most of them for the public interest; and/or CARE - Stress that data sharing and use must benefit the indigenous peoples and the communities that originally 'owned' the data and that these peoples and communities must remain in control.

Ultimately, according to the Data Governance Framework 2.0, data governance is able to create a basis for an environment that builds trust in data-driven technologies. This means that, with the combined data governance approach, **trust principles should be implemented throughout all stages of the extended lifecycle, as shown in the figure below,** presented as a rope of trust conveyed by the combined data governance which runs through all the stages of the extended data lifecycle.

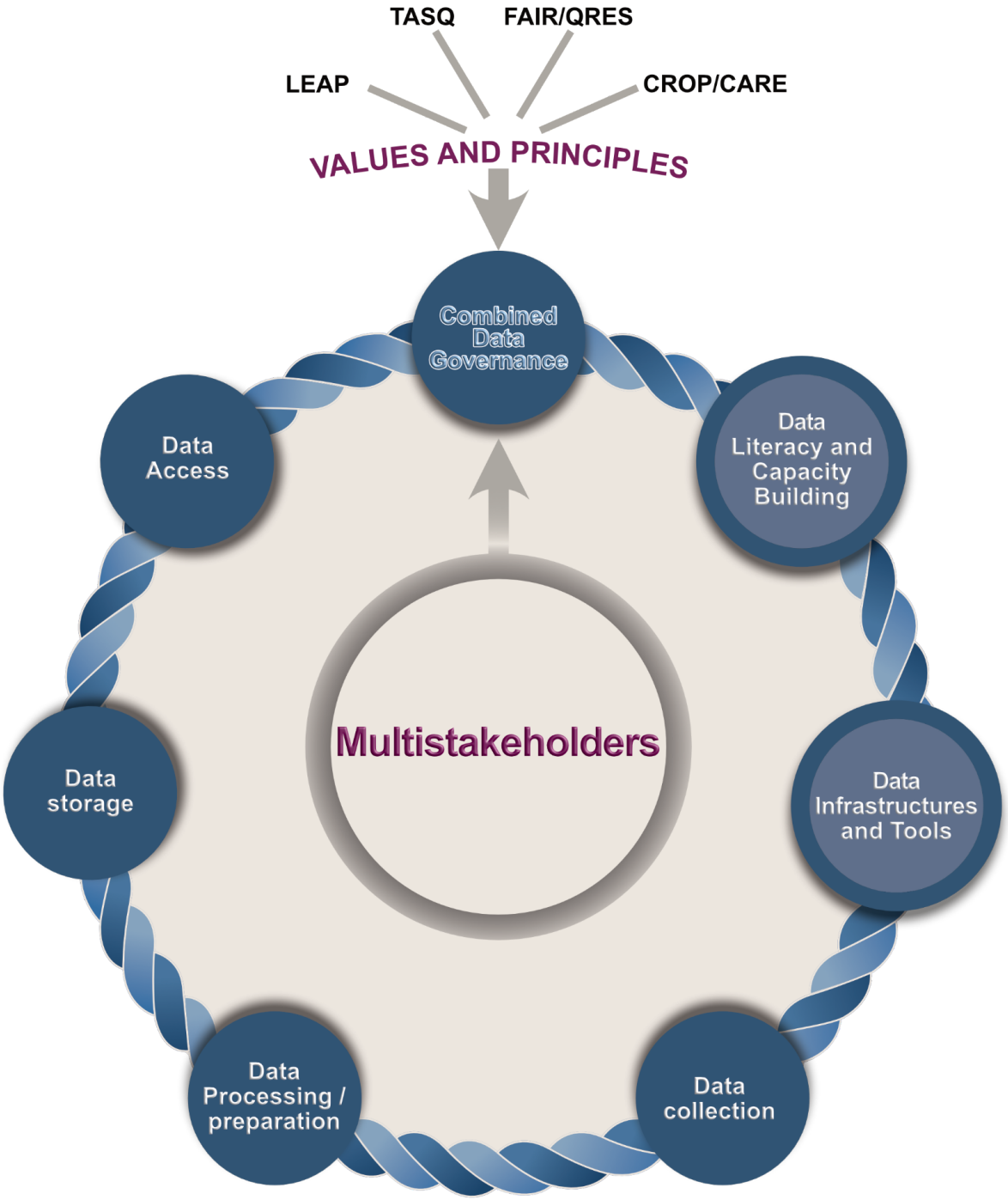


Figure 4 *: The combined data governance approach acting as the rope of trust throughout the extended data lifecycle*

Element 3: Interchangeability of the data stewardship role

Element 2 above shows that data governance is the bond between all stages of the data lifecycle, and that this governance cannot be achieved without the involvement of the various actors, who may be international organisations (NGOs, UN organisations, etc.), local organisations (Governments, NGO, Civil society organisations, etc.), or Citizens. However, the role these stakeholders play in data governance may vary according to the context and domain under consideration.

In the combined data governance approach, the multistakeholder approach portion makes it possible for any organisation to steward data on behalf of others—in this case, the organisation is

known as a data institution[10]. But, it is important to flag that the data stewarding function is not fixed to one particular (or predefined) organisation or actor. In any given situation, an actor may be recognised as a data institution, responsible for collecting, managing or ensuring access to a dataset (i.e. the data steward). In another situation, that same actor may play a role of beneficiary[11], contributor[12], intermediary[13], creator[14], regulator[15] or policymaker[16]. Hence, the notion of ***interchangeability*** is essential to the function of data stewardship between stakeholders of the data ecosystem. In the figure below, bi-directional arrows between data institutions and actors showcase this possible interchangeability.

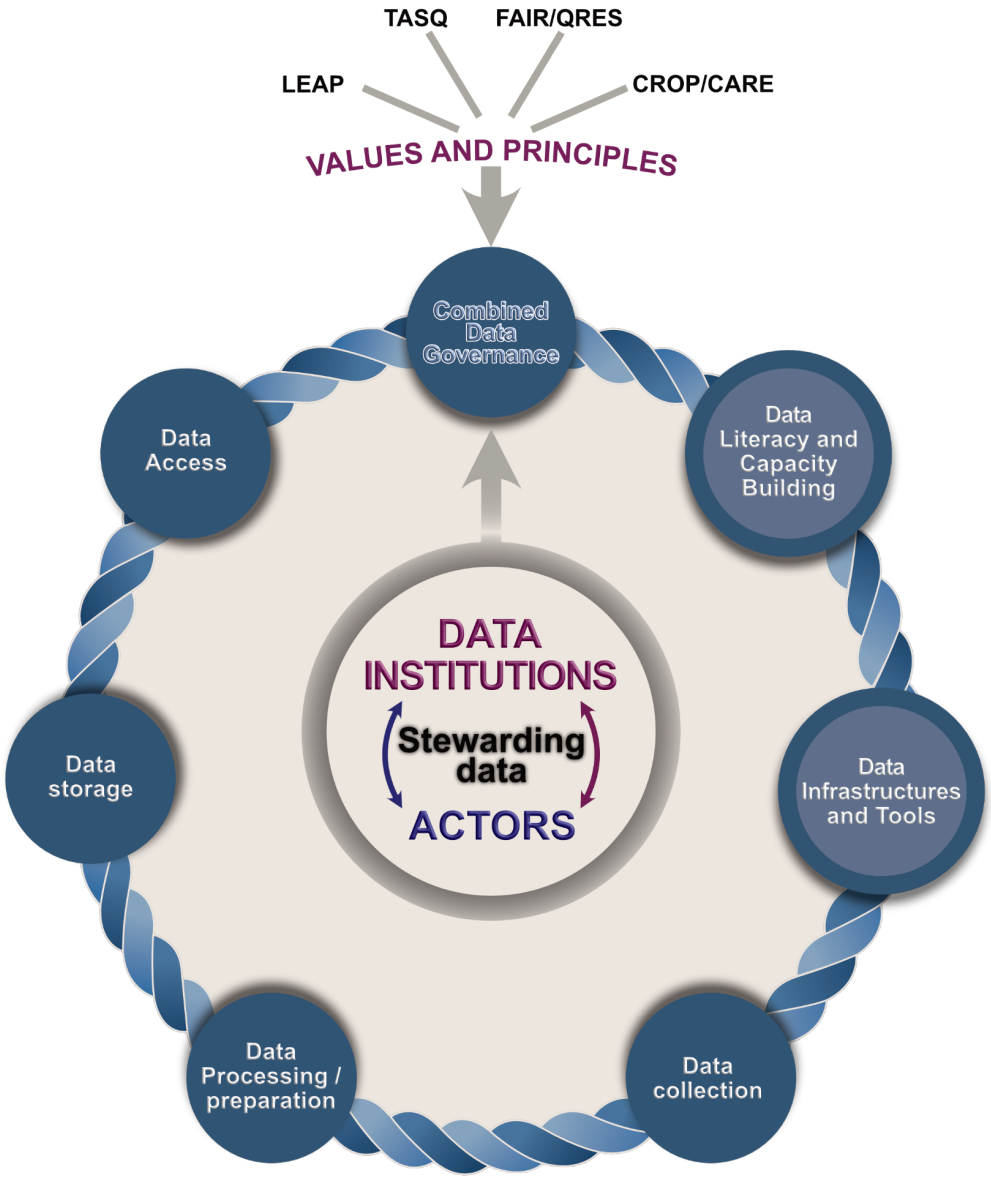


Figure 5 *: Interchangeability of the data stewardship role*

[10] What are data institutions and why are they important?
[11] People or organisations that benefit from the data ecosystem because it enables them to make decisions
[12] The people who contribute to the dataset, either knowingly or unknowingly through use of a service.
[13] Groups that aggregate data in the ecosystem
[14] People or organisations using data to create things (these could be products, services, analyses, insights, stories or visualisations).
[15] Those who create and enforce regulatory frameworks.
[16] Those who create policies, principles and measures.

Element 4: Mechanisms for interaction

The various stakeholders mentioned in Element 3 are not limited to play a specific role; they are instead interacting with and involved in different stages of the extended data lifecycle. Their engagement and responsibilities in data governance are represented in the matrix below:

Table 1 : Matrix of engagement and responsibilities

Data Stewards / Institutions	Diffrerents stage of the data lifecycle	Actors
Should facilitate and afford data literacy to local communities and local organisations	**Capacity building and data literacy**	Have a choice/opportunity to improve their data literacy through training offered by data institutions.
Are in charge of designing, hosting, and maintaining infrastructures	**Data Infrastructures and tools**	Have the opportunity to be part of the co-designing process of these infrastructures
Participate in	**Data collection**	Participate in
In charge of	**Data processing**	Have the option to participate
in charge of	**Data storage**	Have access to data where they are stored
Should share data	**Data access**	Have the opportunity to use, reuse, and share data
Have the opportunity to create new data from existing data	**Data creation**	Have the opportunity to create new data from existing data

Combining the 4 Elements as described, our vision/utopia of trustworthiness in Data Institutions is presented as follows, as the ultimate Trustworthy Data Institutional Framework (TDIF):

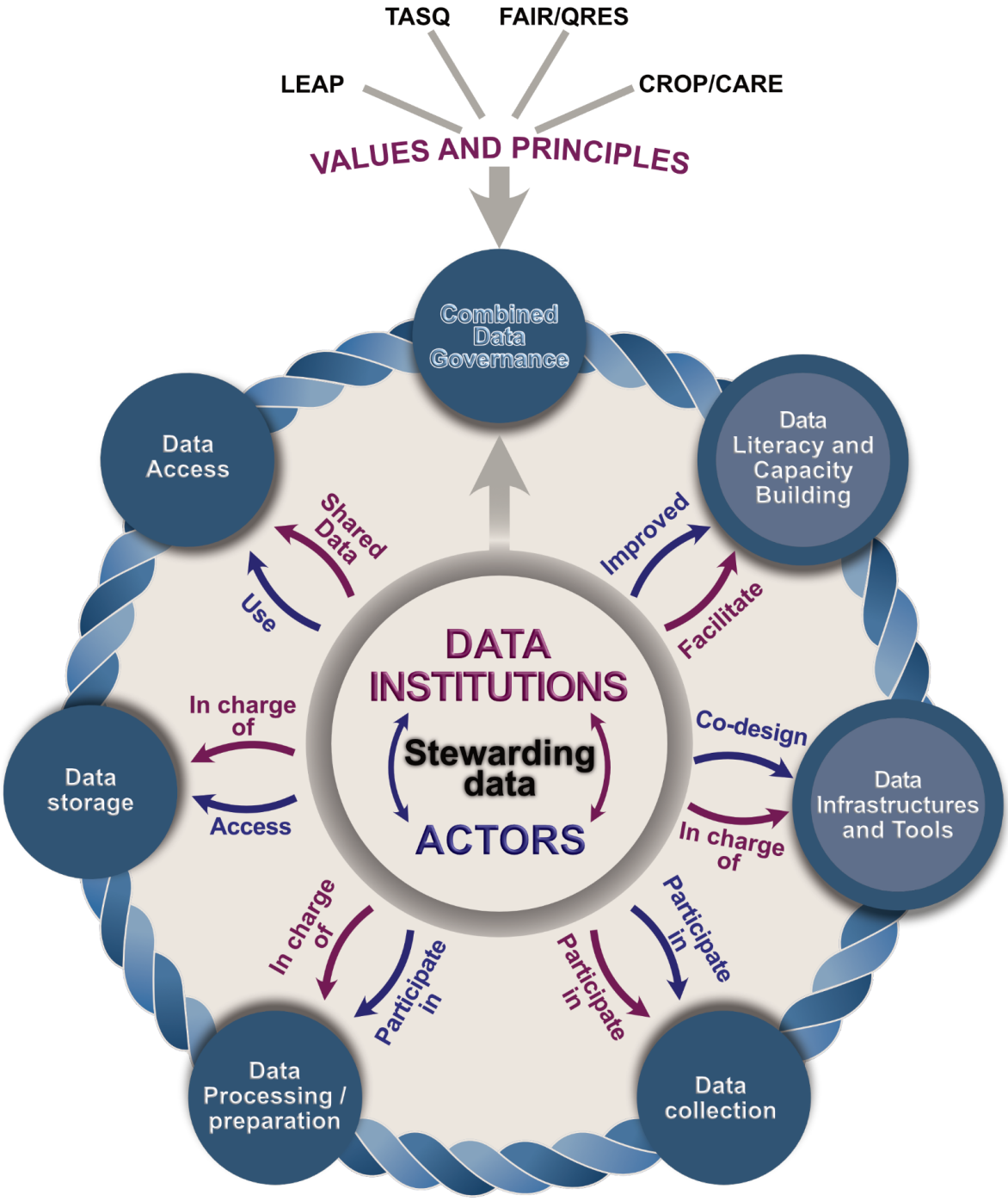


***Figure 6**: Ideal vision of trustworthiness in data institutions - the TDIF*

Trustworthiness Assessment

The TDIF as introduced represents an idealised reality to meet for any data institution. However, achieving this ideal scenario requires a gradual approach, starting with an initial examination of where the organisation stands in terms of trust in their data practices - hence, the importance of assessing trustworthiness.

A Commons-based approach to trustworthiness

While different perspectives of trustworthiness exist, they can be grouped into three main perspectives depending on the capabilities they characterise (technical, ethical, interaction with stakeholders and trust intermediaries) (The Confiance AI Program, 2022, pp. 19–20).

- The **technical perspective** is system-centric, it refers to the ability to verify robust intrinsic properties of data or AI-based components. It allows us to demonstrate the properties of accuracy, robustness, and security. This includes attributes such as reliability, dependability, accuracy, reproducibility, and maintainability.
- The **ethical perspective** is linked to the notion of fundamental rights. It highlights the importance that AI systems operate in full compliance with relevant laws and regulations and comply with ethical principles of human society. This perspective deals with properties such as fairness, privacy, and accountability.
- The **interaction perspective** is linked to notions such as transparency, explicability, and usability.

Due to the different perspectives of trustworthiness, the main challenge when thinking about the application of the TDIF is the need to select one perspective, and to establish appropriate trustworthiness attributes, as their selection is related to the context of application and their nature (either quantitative or qualitative) (The Confiance AI Program, 2022, p. 19).

The TDIF aims to be a practical solution for ethical and responsible governance of data, in the service of economic and social justice. This approach is aligned with the Theory of Commons, and as such, has been selected to use to design the appropriate perspective of trustworthiness.

The Theory of Commons was popularised by the American economist and political scientist Elinor Ostrom, winner of the 2009 Nobel Prize in Economics[17]. This theory places the community at the centre of resources management, and applies when the following four conditions are met: 1) the existence of a resource (data) shared by 2) a community (actors, data institutions) that uses, protects, and maintains it following 3) rules (rights and obligations) that govern the community's use of the resource 4) and a governing structure that ensures the sustainability of the resource and the community that governs it (Ostrom, 1990, 2009). On this basis, we have defined four trustworthiness indicators (Shared Resources, Communities, Rules and Governance) and their variables (attributes).

Trustworthiness indicators and their variables

For each trustworthiness indicator, supplemental variables (attributes) have been identified from various GPAI reports and other well-established resources like the UNESCO Recommendation on the Ethics of Artificial Intelligence[18], and the UNESCO Recommendations on Open Science[19].

[17] https://www.nobelprize.org/prizes/economic-sciences/2009/ostrom/facts/
[18] https://unesdoc.unesco.org/ark:/48223/pf0000380455
[19] https://unesdoc.unesco.org/ark:/48223/pf0000378841

Shared resources

The notion of shared resources here is rooted in the open science perspective and refers to open infrastructures, which could include virtual or physical equipment, sets of instruments, knowledge-based resources, and open computational and data manipulation service infrastructures, that enable collaborative and multidisciplinary solutions which serve the needs of different communities: “Open science infrastructures are often the result of community-building efforts, which are crucial for their long-term sustainability and therefore should be not-for-profit and guarantee permanent and unrestricted access to all public to the largest extent possible” (UNESCO, 2021b). The shared resources indicator includes the following variables:

Table 2 : Description of the shared resources indicator variables

Variables	Description
Equitable access to resources	There is a need to ensure equitable access to skills development and digital infrastructure including connectivity and computing resources, as well as data assets—especially where communities have contributed to the generation of these data assets (GPAI, 2022e, p. 14).
Data infra-structures	Data infrastructures become the open/commons/public part of society’s digital architecture, interrupting its otherwise complete privateness and closedness. It thus provides useful techno-social sites and means for legal and regulatory intervention in digital code and architecture governing our societies (GPAI’s A primer on Data and Economic Justice, 2022, p16).
Safety and security	Unwanted harms (safety risks), as well as vulnerabilities to attack (security risks) should be avoided and should be addressed, prevented and eliminated throughout the life cycle of AI systems to ensure human, environmental and ecosystem safety and security. Safe and secure AI will be enabled by the development of sustainable, privacy-protective data access frameworks that foster better training and validation of AI models utilising quality data (UNESCO, 2021a, p. 7).
Data quality	Degree to which the characteristics of data satisfy stated and implied needs when used under specified conditions. From this point of view data quality depends on the technological domain in which data are used; it is achieved by the capabilities of computer systems' components such as: hardware devices (e.g. to make data available or to obtain the required precision), computer system software (e.g. backup software to achieve recoverability), and other software (e.g. migration tools to achieve portability) (ISO/IEC 25000, 2022).
Usability	Degree to which a product or system can be used by stakeholders to achieve specific goals with effectiveness, efficiency and satisfaction in a specified context of use (The Confiance AI Program, 2022, p. 31).

Communities

This indicator refers to the dynamics around data stakeholders; with value, benefits, and risks of data-driven innovation being distributed equally amongst the communities. The communities indicator includes the following variables:

Table 3 : Description of the communities indicator variables

Variables	Description
Participation	Democratic participation of affected communities requires policymakers to identify the full set of stakeholders who might be impacted by data collection and use, and data-driven activities. The participation of individual and collective data subjects, as well as primary data generators, must be built-in democratically to the design, development and deployment of data intensive systems, including AI (GPAI, 2022e, p. 14).
Re-presentation	The ways in which data is collected and used can have the effect of imposing inappropriate categories and labels onto people, or erasing distinctive identities in data's representation of the world. Data justice calls for us to mitigate and challenge the grouping-together, erasure or omission of identity characteristics which are valued or claimed by people whose data is represented or used (GPAI, 2022b, p. 13).
Data literacy	Capacity building of local stakeholders empowers the creation of local solutions and benefits from locally generated data, and gives local regulators expert knowledge to draw upon to develop local policy solutions that meet local needs. This informs local regulators, and enables sovereign and local community solutions based on community data (GPAI, 2022b, pp. 12–13).
Diversity and inclusiveness	Respect, protection and promotion of diversity and inclusiveness should be ensured throughout the life cycle of AI systems, consistent with international law, including human rights law. This may be done by promoting active participation of all individuals or groups regardless of race, colour, descent, gender, age, language, religion, political opinion, national origin, ethnic origin, social origin, economic or social condition of birth, or disability and any other grounds (UNESCO, 2021a, pp. 6–7).

Rules

Rules indicate the standards by which an organisation governs itself. The rules indicator includes the following variables:

Table 4 : Description of the rules indicator variables

Variables	Description
Data sharing	Advancing data justice calls for the establishment of robust regimes of social licence and public consent, so communities can equitably access and benefit from their data. This includes ensuring the provision of public data infrastructure which allows people not only to port or own their personal data, but to gain access to and beneficially use public data resources (GPAI 2022b, 13).
Transparency	Those with power in processes of collection use of data and data-driven innovation should be obliged to make information publicly available about what data is collected and how it is used, including information about AI inputs, and algorithms, and to provide this information directly to impacted individuals and communities (GPAI, 2022e, p. 15).
National data sovereignty	National data sovereignty as a right of a national community to manage its affairs, including its resources, is enshrined in various international human rights covenants (GPAI, 2022e, p. 15).
Privacy	Privacy as an essential right to the protection of human dignity, human autonomy and human agency, must be respected, protected and promoted throughout the life cycle of AI systems. It is important that data for AI systems be collected, used, shared, archived and deleted in ways that are consistent with international law and in line with the values and principles, while respecting relevant national, regional and international legal frameworks (UNESCO, 2021a, p. 8).
Res-ponsibility and accoun-tability	AI actors and Member States should respect, protect and promote human rights and fundamental freedoms, and should also promote the protection of the environment and ecosystems, assuming their respective ethical and legal responsibility, in accordance with national and international law (UNESCO, 2021a, p. 9).
Societal impact	The continuous assessment of the human, social, cultural, economic and environmental impact of AI technologies should therefore be carried out with full cognizance of the implications of AI technologies for sustainability as a set of constantly evolving goals across a range of dimensions, such as currently identified in the Sustainable Development Goals (SDGs) of the United Nations (UNESCO, 2021a, p. 8).

Governance

This indicator refers to data governance of wider ecosystems, which is the basis for an environment that builds trust amongst society in trustworthy AI-based systems, and other data-driven technologies, helping to facilitate their uptake (GPAI, 2022c). The governance indicator includes the following variables:

Table 5 : Description of the governance indicator variables

Variables	Description
Data commons	Claiming the key resource of data as a commons, and making it equally available to all, ensures much better distribution of economic power, and therefore greater economic justice (GPAI, 2022a, p. 16). Equitable access to data can be achieved through responsible data sharing models such as access to data, or data commons, in managed safe conditions (GPAI, 2022e, p. 14).
Data rights	Based on notions of fairness, a right-based approach to data governance suggests affording data rights to persons or communities that had a share in generating the data (GPAI, 2022e, p. 10). These include: the right to benefit from one's data, and to not be harmed by data collection and use; the right to access and port one's data; the right to appropriate representation in data, including to remaining invisible; the right to participate in governing one's data, and the data systems based on it; the rights to alternative and collective forms of data stewardship (GPAI, 2022e, p. 14).
Data justice	Beyond protecting individual data rights, data justice calls on those with decision making and agenda setting power to actively identify and dismantle the root causes of injustice in and through data practices and systems (GPAI, 2022b, p. 12).
Ownership	Data is a societally-produced resource which has the ability to create enormous value, but ownership and value is concentrated amongst a few powerful firms in the data-driven economy. This is enabled by processes of data extraction, where people and communities are dispossessed of the data they produce, and do not benefit from it. Data justice calls for the economic value of data to be shared equitably across and within countries (GPAI 2022b, 13).
Intellectual Property Rights (IPR)	Building a dataset requires many processes such as collecting/recording, cleaning, filtering, labelling, and/or aggregating by data scientists. Most of them will be annotated. Such a dataset can be built by an individual or a company collecting its own data (for example, operating data of its factories) or can be licensed. Protecting such a dataset with IPR could create an incentive to create high-quality datasets (GPAI, 2022f, pp. 15–16).
Policies	Policymakers should continue to embrace a "risk-based and proportionate" approach to AI regulation. This recognises that AI covers a wide range of use cases and technologies, and this approach should help to ensure that the regulatory requirements for an AI system are commensurate with its risk profile (Catherine Gray, 2022).

The TDI-Maturity Tool

This systematic tool has been designed as part of this work to facilitate trustworthiness assessment inside data institutions. It incorporates maturity levels, an evaluation grid, and a scoring methodology.

Maturity levels

The maturity level refers to the stage an organisation has reached in implementing and adopting data trustworthiness. The maturity levels in use here are inspired by the data maturity framework (Data Orchard, 2022), the data governance maturity (Ovaledge, 2021) and the Capability Maturity Model Integration (CMMI) approaches (CMMI Institute, 2019). In all, there are five maturity levels:

Table 6 : Definitions of each level of maturity

Unaware (initial, nascent)	Emerging (aware)	Learning (defined, proactive:)	Developing (implemented, managed) :	Mastering (optimised, effective)
Unaware of the importance of data	There is an awareness of the importance of data	Data governance rules and policies are defined	Data governance policies and implementing rules are enforced	Rules and policies for better efficiency are optimised
Limited to no data processes or governance	Existing data practices are understood and well documented	Data owners and data stewards are identified	There is training conducted	Clear and comprehensive data management principles are adopted organisation-wide
The absence of data owners is apparent;	Several data projects, such as mapping data infrastructure, are underway	Some data stewards have been identified and appointed	Data policies are well-defined	Everything in the developing level is optimised.
There is no data governance, data ownership, or accountability in place	Policies have been created but adoption is low	A governance committee is set up	Well-defined data quality goals are in place	
There are no formal procedures for tracking data	Everything in the unaware level is improved.	Data policies are well-defined	Data governance principles drive all data projects	
There are no processes or architecture in place for information sharing		Users are sharing and understanding data management processes	Data policies have been developed, initiated and are well understood	
		Data stewards and owners are identified and active	A data governance body has been created	
		Everything in the emerging level is considered.	Everything in the learning level is applied.	

Scoring methodology and evaluation grid

For calculation purposes, two different interval scales[20] will be used.

- For variables the scale is: Unaware [0 to 1], Emerging [2 to 3], Learning [4 to 5], Developing [6 to 7], Mastering [8 to 9]. For each variable, refer to its description in Appendix A, then:
    - Identify the description of the level of maturity that is closest to your organisation's situation;
    - After discussion within the group, assign a consensus score corresponding to the range of maturity levels in which you have categorised your organisation.
- For each indicator, the sum of the scores of its variables will enable us to obtain the indicator score. The score is then converted into a percentage, so that an interval scale can be applied to rate the indicators.
    - Depending of the percentage obtained, maturity level of the indicator is assigned as follows: Unaware [0 - 20%], Emerging [20% - 40%], Learning [40% - 60%], Developing [60% - 80%], Mastering [80% - 100%];
    - Based on the maturity level of each indicator, use Appendix B to take concrete actions in order for your organisation to move to the next level of maturity.

By combining the two scales emerges the following evaluation grid to be used by organisations wishing to assess their trustworthiness.

[20] For the interval scale, the distances between numbers have meaning. You can categorise, rank, and infer equal intervals between neighboring data points. Attributes on an interval scale have the following property: they have a natural order. We can compute their mean, median, mode, and standard deviation. They have an exact difference between values. ” (Confiance AI, 2022; p21).

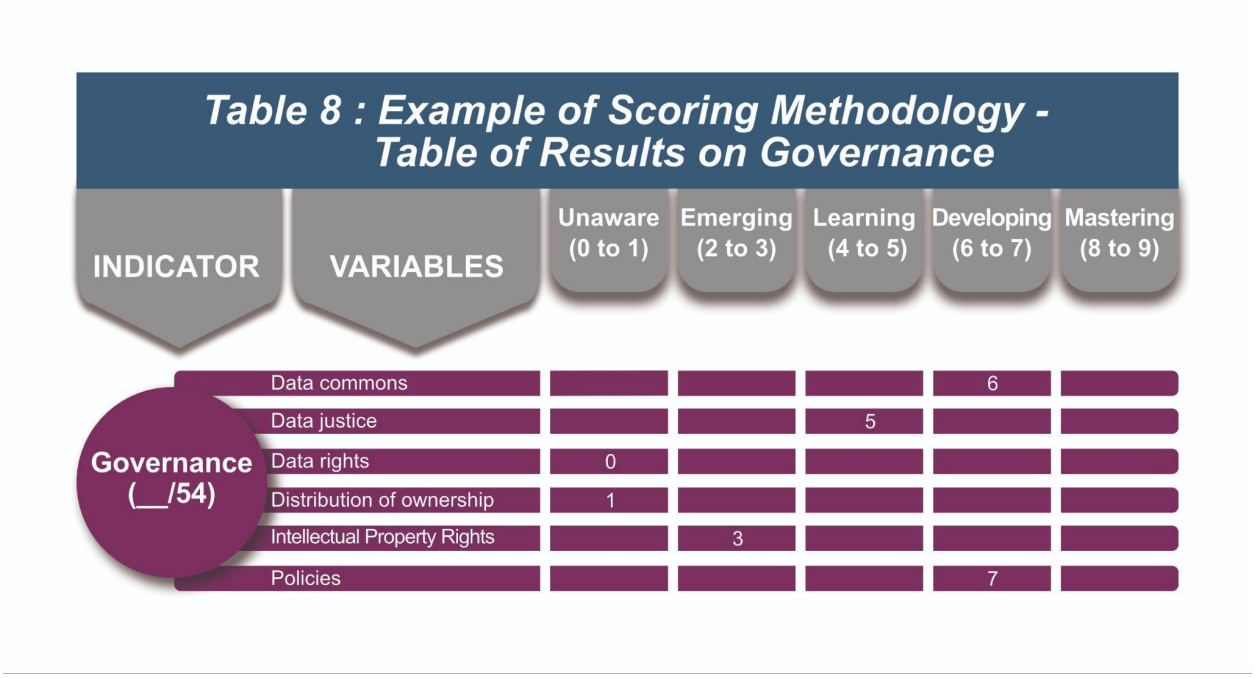
Table 7 : Evaluation grid

INDICATOR	VARIABLES	Unaware (0 or 1)	Emerging (2 or 3)	Learning (4 or 5)	Developing (6 or 7)	Mastering (8 or 9)
Shared resources (__/45)	Equitable access to ressources					
	Data infrastructures					
	Safety and security					
	Data quality					
	Usability					
Community (__/36)	Participation					
	Representation					
	Data literacy					
	Diversity and inclusiveness					
Rules (__/54	Data sharing					
	Transparency					
	National data sovereignty					
	Privacy					
	Responsibilities and accountability					
	Societal impact					
Governance (__/54)	Data commons					
	Data justice					
	Data rights					
	Distribution of ownership					
	Intellectual Property Rights					
	Policies					

NB:

- *We are not assigning a weighting coefficient or a priority to our variables and indicators, as we consider them to be of equal importance.*
- *For a practical session on the TDIF, please use the printable version of the evaluation grid found in Appendix D.*

Example utilising the governance indicator



Steps:

1. The overall governance score is calculated as: $\frac{(6+5+0+1+3+7)}{54} = \frac{22}{54} = 40.7\%$
2. This percentage score means that for the Governance indicator, this particular organisation is at the 'Learning' stage of maturity;
3. The organisation should take actions to move their governance processes from the 'Learning' stage towards the 'Developing' stage;
4. The organisation would then continue the same process for the remaining indicators.

Conclusion

The TDIF aims to be a practical solution for ethical and responsible governance of data, in the service of economic and social justice. The TDIF does not intend to ask organisations to create a new body regulating trust; but instead, it aims to allow organisations to build their capacities in those areas needed to improve trust. With the TDIF, one can analyse current data practices within an organisation, identify gaps and develop the strategy needed to meet the requirements for more trust and inclusion of local communities.

The TDIF is a tool for anyone who wants to adopt safe, fair, inclusive, and equitable collection, sharing, and use of data within and between organisations. In general, these organisations are:

- international organisation stewarding data, to evaluate the level of trust and inclusion in their data workflow and build trust through an effective engagement of local communities;
- national organisations stewarding data, to evaluate the level of trust in their data workflow and to develop tools ensuring interoperability with international organisations. This will allow them to claim their ownership when data are collected locally and to ensure accessibility to citizens;
- Governments, to develop policies ensuring that the outputs of data benefit first the local populations and their country;
- civil society organisations, to allow them to better position themselves, participate in decision making, and educate citizens in the responsible use of the data to which they have access; and
- citizens, to help them know what data they have access to, claim their rights to data, and best utilise the data collected from them.

In summary, at the dawn of an AI-driven future, where data is managed with the utmost integrity and accountability, this report offers the TDIF as an useful blueprint. Rather than simply promoting trust, the TDIF deepens the foundations that support it, providing a true foundation on which responsible AI can be built. Serving a wide range of stakeholders, from global entities to individual citizens, the TDIF paves the way for transparent and inclusive data practices. By giving voice to local communities, championing citizens' rights, and building connections, TDIF not only strengthens our shared commitment to fairness and justice in our digital world, but also paves the way for an AI ecosystem that is ethical, equitable, and truly beneficial to all.

Bibliography

Catherine Gray. (2022). Lee Tiedrich on the importance of regulations for AI policy. *AI Strategy*.

CMMI Institute. (2019). *The Data Management Maturity (DMM) Model*.

Data Orchard. (2022). *Data maturity framework for the not-for-profit sector*.

GPAI. (2021a). *Data Governance Working Group Report*.

GPAI. (2021b). *Enabling data sharing for social benefit through data trusts*, An Interim Report for the 2021 GPAI Paris Summit.

GPAI. (2022a). *A Primer on Data and Economic Justice*, Report, November 2022.

GPAI. (2022b). *A Primer on Data and Social Justice*, Report, November 2022.

GPAI. (2022c). *Data Governance Working Group: A Framework Paper for GPAI's Work on Data Governance 2.0*, Report, November 2022.

GPAI. (2022d). *Data Governance Working Group Report*, Report, November 2022.

GPAI. (2022e). *Data Justice Policy Brief: Putting Data Justice into Practice*, Report, November 2022.

GPAI. (2022f). *Protecting AI innovation, Intellectual Property (IP): GPAI IP Primer*, Report, November 2022, Global Partnership on AI.

GPAI. (2023). *Designing Trustworthy Data Institutions: Scanning the Local Data Ecosystem in Climate-Induced Migration in Lake Chad Basin - Pilot Study in Cameroon*, Report, October 2023, Global Partnership on AI.

ISO/IEC 25000. (2022). *Quality of data product*. ISO 25000 Portal.

ODI. (2021). *Trustworthy Data Stewardship Guidebook BETA*.

Ostrom, E. (1990). *Governing the commons: The evolution of institutions for collective action*. Cambridge University Press.

Ostrom, E. (2009). *Beyond Markets and states: Polycentric governance of complex economic*. Nobel prize lecture.

Ovaledge. (2021). *Data Governance Maturity Models and How to Measure It?*

The Confiance AI Program. (2022). *Towards the engineering of trustworthy AI applications for critical systems.* Confiance AI.

UNESCO. (2021a). *Recommendation on the Ethics of Artificial Intelligence*.

UNESCO. (2021b). *UNESCO Recommendation on Open Science*.

Appendix A: Description of variables by levels of maturity

SHARED RESOURCES *Variables: Equitable access to resources, Data infrastructures, Safety and security, Data quality, Usability*				
UNAWARE	**EMERGING**	**LEARNING**	**DEVELOPING**	**MASTERING**
EQUITABLE ACCESS TO RESOURCES				
• Data only accessible to a single person or team, usually junior staff	• Starting to find out what data is available internally. Know where most data assets are but there may be more squirrelled away in parts of the organisation	• Users are sharing and understanding data management processes • Open datasets are occasionally used	• Data and analysis is becoming more available and accessible to actors of the local data ecosystem; though may require some intervention by specialists to provide this.	• Tools able to access and utilise internal and external data directly, for both experts and non-experts • Everyone can access the analysis they need when they need it.
DATA INFRASTRUCTURES				
• Data is mostly collected via paper, email, SMS messages. This may not get transferred onto spreadsheets or structured document filing systems	• Data is stored in designated physical locations, in paper and digital formats, in organised ways • Data is mostly collected on paper/ phone/in person and then entered into a database or spreadsheet for basic analytical and reporting tasks • Tools are limited, may not be up-to-date, don't meet current needs, and are not documented or supported • Tools are acquired on a 'needs-must' basis e.g. for a specific purpose/project or when a crisis/system failure occurs • Joining data or analysis across teams/services/functions requires manual exporting and re-stitching	• Unstructured data is becoming better organised and searchable (e.g. folder structures/file naming conventions) • Possible advanced analytical tool used for basic data processing or descriptive statistical analysis • Tools likely to be purchased or built as 'one-offs' for specific purposes with limited flexibility for change or improvement • There is some data management technology in use • A data integration plan is being worked on • In house or externally provided training for using data systems.	• Data held in appropriate databases accessible by expert users and some non-experts • Data is collected and automatically stored digitally wherever possible e.g. online forms/apps directly into databases • An inventory of tools and systems (including hardware, software, licence, passwords and access) is managed and maintained • Most tools are up to date with support available • Advanced tools being used for sophisticated analytics in some parts of the organisation e.g. R, SAS, SPSS, Python	• The organisation has a robust infrastructure, integrating tools wherever possible • Data fully centrally stored in secure digital systems with managed access • Active in online learning networks and data and analytics communities of practice exploring new tools and skills.
SAFETY AND SECURITY				
• There are no formal procedures for tracking data	• Start to understand the need for data protection, but responses are reactive and inconsistent	• Data quality risk assessment measures are in use • Data protection and security policies are in place	• Regular audits are conducted to identify and address vulnerabilities • The organisation goes beyond legal requirements to ensure data security	• Systems, automated if possible, in place to delete personal data no longer necessary and respond to subject access requests

SHARED RESOURCES

Variables: Equitable access to resources, Data infrastructures, Safety and security, Data quality, Usability

UNAWARE	EMERGING	LEARNING	DEVELOPING	MASTERING
• Minimal, if any, security and protection of data on paper, computers, or devices • Lack of any form of data protection practices • There is no awareness or acknowledgment of the necessity to protect data, potentially leading to significant vulnerabilities and risks • Little or no staff awareness or training in data protection and security • No steps to ensure the accuracy, relevance, and security of the data it collects	• Some basic protective measures, such as password protections or firewall use, but these measures are not systematically implemented or updated • Data may be shared mostly by emailing spreadsheets and documents as attachments with duplication, version control, and security issues • Start improving data security,	• Digital data is mostly centrally stored on a (secured, backed-up) cloud-based system or local server with managed access. Some may remain inaccessible on computers, central shared drives or devices • Compliance with applicable data protection laws is ensured • Staff have basic data protection and security training though they might not be very confident	• High levels of confidence about the security of data held in the organisation • Staff know how to respond to a data breach, potential breach, or near miss.	• Risks monitored and tested to improve data security and protection • Continuous improvement of data protection measures, using feedback from stakeholders, audits, and industry best practices
DATA QUALITY				
• Limited data (if any) collected • Collected manually, mostly on paper, only when needed for specific purpose • Not checked for validity or accuracy • Nobody is aware or interested in the data assets in the organisation • Data is disorganised and unmanaged and stored in a range of places: on desks, in filing cabinets, individual peoples' email inboxes, computers, phones, or other devices	• Data collection is both on paper and in digital forms though there may be inconsistencies and inefficiencies in approach • Data is rarely updated and cleaned • A data quality strategy is defined, approved, and managed	• Though errors remain, data collection methods and processes are being improved • Data is reviewed to assess how relevant, meaningful, and necessary it is • The organisation knows how good or bad its different data sets are; and knows which data sources can/can't be trusted • Gaps, overlaps, and mismatches in the available data have been identified • All data assets are known but may not be formally recorded	• Data requirements defined and consistently collected via a range of methods • Data is monitored for quality including completeness, accuracy, and validity. Tools and systems exist for cleaning and maintenance • Richer data collection with more integration/alignment between systems reduces duplication, inefficiency and error • Data quality metrics are employed to analyse proposed changes to the data quality strategy • Well-defined data quality goals are in place	• Monitors and fully understands the quality of the data it holds and hence has high levels of confidence and trust in its data • Commissions external independent research and evaluation • Maintains full inventory of data assets across the whole organisation with clearly defined variables, ownership, review periods, and development plans for each • Data quality program milestones and metrics are regularly reviewed by executives, and continuous improvements are implemented
USABILITY				
• Collect and use data for requisite purposes e.g. basic financial management and legal/funder/contract compliance reporting	• Several data projects, such as mapping data infrastructure, are underway • There is a small degree of automation	• Building internal knowledge and expertise based on the analysis of data and dialogue on how to act on this	• Data is starting to be used to inform efficiency savings (resources, processes and service/product design)	• Data is used extensively, and in inter-related strategic ways, for a wide range of purposes • Sophisticated use of analysis delivers insights and predictions to

SHARED RESOURCES *Variables: Equitable access to resources, Data infrastructures, Safety and security, Data quality, Usability*				
UNAWARE	**EMERGING**	**LEARNING**	**DEVELOPING**	**MASTERING**
• Data isn't meaningful or useful to the organisation		• Strategic planning, particularly around efficiency and service development, is becoming more data informed	• Strategic planning and decision making is becoming considerably data informed • Statistical analysis reports for process, reporting, and performance are included in the metadata repository and employed to support fact-based decision making for new metadata management initiatives	influence service and organisational success • Use data to increase efficiencies (resources,processes,services/product delivery) • Strategic planning and decision making is highly informed by data and based on past, present and future analyses • Users tag data to increase discoverability

COMMUNITIES *Variables: Participation, Representation, Data Literacy, and Diversity and Inclusion*				
UNAWARE	**EMERGING**	**LEARNING**	**DEVELOPING**	**MASTERING**
PARTICIPATION				
• No local communities commitment beyond basic data collection tasks. • Responsibility for data collection and control is at the funder/data institutions level.	• Some dedicated person from the local communities can collect, manage and use data within other roles	• Local communities become engaged, supportive, ask the right questions of the data, and active in harnessing its value. • Some data insights are shared with local communities, and in the public domain	• Data seen as a team effort and critical asset for every part of the data ecosystem. • Regular use of local communities expertise.	• Everyone in the data ecosystem is committed to ensuring quality data is available to support decision-making.
REPRESENTATION				
• Unaware of the importance of having local communities of the data ecosystem represented in data governance.	• Little awareness of the potential of local communities, but don't value it.	• People across the organisation are starting to talk about how they can work with local communities to deliver better data for decision making	• Local communities are starting to be recognised as important at a more senior level.	• Establishing relationships with local communities for support and advice, mostly around specific tools, systems or projects with some skills development
DATA LITERACY				
• Local communities are not interested in data and there is little or no internal skills, training, or expertise. • Organisations don't really understand the needs and skills required for building data capabilities of local communities.	• Organisation offers Basic/adequate skills and training in using data for local communities; • Limited or very basic data and analytics knowledge and experience among leadership	• Beginning to understand needs around data skills and capabilities of local communities • Organisation adopt the commitment to improving data literacy of local communities.	• Increased data literacy across the organisation. • Possibly a senior person/team bringing organisation-wide data together. • Understand different skill sets within data ecosystem;	• All staff trained with ongoing investment in developing data skills with high levels of data literacy across the organisation. • Specialist staff regularly update skills and knowledge through training and conferences.
DIVERSITY AND INCLUSION				
• Not interested in local communities at all;	• Little awareness of the potential of local communities, but do not see their inclusion as a priority.	• People would like to share more but may be constricted by access/permissions/cultural barriers.	• Becoming engaged, supportive, asking the right questions of the data, and active in harnessing its value.	• Senior data strategist and local communities representatives are embedded at heart of leadership decision making

RULES *Variables: Data sharing, Transparency, National data sovereignty , Privacy, Responsibility and accountability, societal impact*				
UNAWARE	**EMERGING**	**LEARNING**	**DEVELOPING**	**MASTERING**
DATA SHARING				
• Data is never shared internally or externally. • No data sharing happens in the organisation. • Organisation's culture doesn't encourage data sharing across teams, though this may occur occasionally verbally or via reports.	• Agreements are in place that provide explicit expectation for the use of shared staff resources with responsibilities for data management. • Some people or teams may use cloud-based storage to share some data (e.g. OneDrive, Google Drive, Dropbox, Box). Note these may be personally or organisationally owned.	• People would like to share more but may be constricted by access/permissions/cultural barriers. • Some data insights are shared with partners, networks, and in the public domain.	• External data sharing is done on an aggregated basis and insights are shared including some shared measures and benchmarks. • Exploring how data could be shared with actors of the local data ecosystem, on an individual basis as part of service delivery.	• Data insights/evidence publicly available. • Extensive data sharing, with protocols in place with partners, networks, stakeholders to address shared problems and solutions. • Sharing data internally from different teams, departments and services is becoming the norm.
TRANSPARENCY				
• Little to no information about how personal data is collected, used, and shared • Lack of formal data handling practices or they may not be communicated clearly to users • No transparency about data practices	• Organisation recognize the importance of data transparency and take initial steps toward improving practices • Start informing users about data transparency practices • Data transparency practices may not be thoroughly enforced or consistently applied	• Data management processes are established and maintained by the data management function with governance approval • Regularly communicate about their data practices to their users • Data management objectives, priorities, and scope are defined and approved.	• Having comprehensive data handling practices • Organisations proactively communicate their practices to users in a clear and accessible way • Seek to engage with users, seeking feedback and offering avenues for users to manage their own data • Prioritise transparency	• Internal openness and data sharing is fundamental to the culture, subject to data protection/security. • Fully embed data transparency into their culture and operations • Proactive in keeping users informed about any changes or incidents • Continuously evaluate and improve their practices, based on feedback, audits, and assessments
NATIONAL DATA SOVEREIGNTY				
• The nation does not recognize the strategic importance of data sovereignty. • Data is often stored, processed, or managed by external entities without proper oversight or governance.	• Awareness of data sovereignty issues exists, but actions are typically reactive. • The nation might implement ad-hoc measures in response to specific incidents or challenges. •	• The nation starts developing and implementing comprehensive policies and regulations to govern data usage, storage, and transmission. • There's an active push for domestic data storage or at least clear regulations for cross-border data transfers.	• Advanced infrastructure exists domestically for data storage, processing, and management. • Regulations are well-established and are harmonised with global standards where necessary. • Active participation in international data governance dialogues.	• The nation is not just safeguarding its own data sovereignty but also setting global standards and best practices. It may have a thriving domestic tech industry that innovates in areas of data security, privacy, and governance. • The country might also offer solutions and frameworks for other nations to emulate.

RULES

Variables: Data sharing, Transparency, National data sovereignty , Privacy, Responsibility and accountability, societal impact

UNAWARE	EMERGING	LEARNING	DEVELOPING	MASTERING
PRIVACY				
• The organisation does not recognize or respect the right to privacy. • Personal information are collected, used, or disclosed without consent or justification, • Compliance with data privacy regulations is likely minimal or non-existent • Not fully compliant with data protection regulations	• Start to acknowledge the importance of privacy, but its actions are reactive and inconsistent. • Actions are taken to protect privacy in response to legal requirements or specific incidents, but it does not have a comprehensive privacy strategy. • Taking steps towards compliance with data protection laws.	• May have a dedicated privacy officer or team to handle these issues • Compliance with applicable privacy laws and regulations, • Work on complying with applicable data privacy laws • Take proactive steps to protect privacy and ensure data accuracy.	• Systems have been created to ensure data about identifiable individuals is deleted when no longer necessary and respond to subject access requests. • Actively works to improve its privacy practices, including through regular audits and updates to its policies and procedures. • Committed to complying with, or even exceeding, data privacy regulations	• The organisation continuously works to enhance privacy protections, using feedback from stakeholders, audits, and best practices. • Advocating for stronger data protection laws or sharing its best practices with others • Go beyond legal compliance, striving for best practices in data handling • All relevant staff are trained on data protection practices
RESPONSIBILITY AND ACCOUNTABILITY				
• Data is seen as the responsibility of 'someone else', usually in an administrative role • Nobody has any formal responsibility for managing any data in their job. Any organising, archiving, updating or data cleaning is performed in an ad hoc way by individuals • There's no acknowledgment of the need for data accountability.	• Recognize the importance of data responsibility and take initial steps towards it. • Start to realise the importance of data accountability, but actions are inconsistent and reactive rather than systematic.	• A data management strategy representing an organisation-wide scope is established, approved, promulgated, and maintained. • Roles and responsibilities for governance, implementation, and management of data quality practices are defined. • There's a designated person or team responsible for data accountability.	• People are formally responsible for managing the storage, cleaning and maintenance, security, and backup of all data. Where possible this is becoming routine and/or automated. • Data accountability is embedded into the organisation's strategy and operations. • Training on data accountability is provided to key stakeholders • Dedicated skilled analytics roles established with several people responsible for data in different roles/ teams.	• Data responsibility is fully integrated into the organisation's culture and operations. • Data accountability is a key part of the organisation's culture and is consistently prioritised across all levels of the organisation. • There are robust processes for monitoring and improving data accountability practices, including regular audits and feedback mechanisms. • Actively engages with stakeholders on data accountability issues
SOCIETAL IMPACT				
• No awareness or consideration of societal impact. • Data practices are driven purely by operational needs.	• Recognition of the importance of societal impact. • Initial frameworks or guidelines are in place to mitigate negative consequences.	• Collect data to be able to understand and evidence the communities needs and problems the organisation addresses • Active strategies to ensure data practices benefit society. Consistent evaluations of societal implications.	• A data management organisation and specified structure are defined and periodically reviewed to ensure that they meet the needs of local communities. • Societal considerations are embedded in all data activities.	• Fully understand how to use data to improve the community life; • Leading practices in societal engagement. • Data-driven initiatives shape societal standards and contribute to global challenges.

RULES *Variables: Data sharing, Transparency, National data sovereignty , Privacy, Responsibility and accountability, societal impact*				
UNAWARE	**EMERGING**	**LEARNING**	**DEVELOPING**	**MASTERING**
		• Collaborative engagements with stakeholders.	• Active partnerships with external entities to achieve societal goals. • Emphasis on sharing findings and data-driven insights for societal good.	• Emphasis on constant innovation and evolution in societal impact strategies.

GOVERNANCE

Variables: Data commons, Data justice, Data rights, Distribution of ownership, Intellectual property rights, policies.

UNAWARE	EMERGING	LEARNING	DEVELOPING	MASTERING
DATA COMMONS				
• Limited to no data processes or governance • Data management is ad-hoc and reactive	• A defined and documented data governance structure is in place • A review process is established and followed to evaluate and improve data governance • Data teams are beginning to focus on metadata	• A governance committee is set up • Some data stewards have been identified and appointed • Existing data practices are understood and well documented	• Board and senior management keep abreast of current legislation and best Practice	• Clear and comprehensive data management principles are adopted organisation-wide
DATA JUSTICE				
• No awareness of data fairness issues • Data are collected, processed, and used without considering the potential for bias, discrimination, or unequal treatment of individuals or groups	• An approved interaction and engagement model ensures that stakeholders engage with the data management organisation. • Some measures are taken to address fairness, such as attempting to remove biased data or improve the diversity of data sets, but these measures are not systematic or consistent • Users are aware of the business value of data • Start to recognize the importance of data fairness, but responses are reactive and sporadic	• Principles are defined and followed to guide the consistency of practices related to data management • Data fairness principles are embedded in the organisation's data practices • Regular audits are performed to detect and correct bias in data and algorithms • Use of techniques to mitigate bias in machine learning, and to ensure the diversity and representativeness of data • There may be efforts to audit data and algorithms for fairness	• Data fairness principles are embedded in the organisation's data practices • Regular audits are performed to detect and correct bias in data and algorithms • Staff know how to respond to subject access requests (where individuals request a copy of their data) or changes in preferences on personal data. • Fairness is considered in all stages of data collection, processing, and use • Training on data fairness issues is provided to relevant staff	• Data fairness is a key part of the organisation's culture and operations • The organisation goes beyond compliance with legal requirements and actively seeks to promote fairness • Existing robust processes for monitoring and improving data fairness practices • Actively engages with stakeholders, including those who are affected by its data practices
DATA RIGHTS				
• individuals have no control over their data. • The organisation or system lacks awareness of data rights. No clear policies, practices, or procedures related to data rights.	• Awareness of data rights exists, but practical implementation is minimal. Initial discussions about embedding data rights might begin. •	• Provides some level of control to individuals over their personal data • Active efforts to document and establish policies related to data rights. Introduction of protocols for data access, portability, and potential benefits sharing.	• Data rights are integrated into daily operations. Clear channels for individuals to access, port, correct, or delete their data. Participation mechanisms are introduced.	• Comprehensive data rights management, including innovative methods of collective stewardship, community participation, and broadening the understanding of data rights. Active monitoring and adjustments based on feedback and evolving standards.

GOVERNANCE *Variables: Data commons, Data justice, Data rights, Distribution of ownership, Intellectual property rights, policies.*				
UNAWARE	**EMERGING**	**LEARNING**	**DEVELOPING**	**MASTERING**
DISTRIBUTION OF OWNERSHIP				
• There is no data ownership in place • The absence of data owners is apparent	• Some data is managed and controlled by people with clear responsibility for maintenance and cleaning • Data is seen as the responsibility of 'someone else', usually in an administrative role	• Data owners and data stewards are identified • Some data is managed and controlled by people with clear responsibility for maintenance and cleaning	• People are formally responsible for managing the storage, cleaning and maintenance, security, and backup of all data. Where possible this is becoming routine and/or automated	• Range of people with senior management keep abreast of future changes in legislation and best practice, and regularly check Data Protection compliance
INTELLECTUAL PROPERTY RIGHTS				
• No recognition of data as an intellectual asset. No policies regarding IP protection of data sets.	• Recognizes the importance of data but has no structured IP strategy for data governance. Reactive approach to data-related IP issues. • Occasional protection against data misuse, but largely inconsistent and fragmented approach	• Initial frameworks in place to identify and categorise data that could be deemed intellectual property. Basic guidelines for data sharing, licensing, and protection. • Clear policies and strategies to govern data as IP. Regular training and updates on data-related IP matters. Consideration of licensing or sharing agreements for datasets.	• Data governance and IP strategies are intertwined. Emphasis on not just protecting data but also maximising its value through strategic partnerships, licensing, or data-driven innovations.	• Leading practices in data IP management. Actively shapes data IP standards in the industry. Recognizes global nuances in data IP and crafts strategies accordingly. Engages in proactive measures to ensure that data assets remain protected and optimised for future innovations.
POLICIES				
• There are no policies related to data • Lack of clear policies and procedures for handling data	• Basic policies for data protection and security may be in place but not monitored or enforced • Start developing and implementing data handling policies	• Data governance rules and policies are defined • Data policies are well-defined • Policies and processes to promote data fairness are established • The organisation has established data protection policies and procedures, which may include measures like regular data backups, encryption of sensitive data, and user access controls	• Data governance policies and implementing rules are enforced • Data policies are well-defined • Policies and practices are well established to ensure data is safeguarded (e.g. rules on passwords, how data is stored, rights/privileges to access organisational and client data) • Regularly reviews and updates established policies and procedures • The organisation has established policies, processes, and guidelines to implement the data quality strategy	• Rules and policies for better efficiency are optimised • The policies, processes, and governance contained in the data quality strategy are anchored across the data lifecycle, and corresponding processes are mandated in the system development lifecycle methodology • Having established and implemented data handling policies and procedures • The organisation has established clear policies and procedures for protecting privacy

GOVERNANCE *Variables: Data commons, Data justice, Data rights, Distribution of ownership, Intellectual property rights, policies.*				
UNAWARE	**EMERGING**	**LEARNING**	**DEVELOPING**	**MASTERING**
			• Standard data governance policies and processes are followed	• the organisation has established clear policies and procedures for data accountability

Appendix B: Actions to take to improve trustworthiness

FROM UNAWARE TO EMERGING
• Audit how data is shared in their organisation and create a plan that includes data owners and other stakeholders. • Dismantle structural and historical inequality, by acknowledging the inherent biases in data creation and collection. • Educate stakeholders of the data ecosystem and specifically, local communities about the importance of data governance and focus on the potential implications of breaching compliance regulations.
FROM EMERGING TO LEARNING
• Identify and analyse potential problems to take necessary corrective measures. • Ensures that the organisation understands, maps, inventories, and controls its data flows throughout the entire lifecycle. • Discuss access to data, considering both individual actors and the broader societal implications, particularly for civil society and academia. • Adopt a basic data rights framework, emphasising core rights related to access, representation, and governance. • Define the vision, goals, and objectives for the data management program, ensuring alignment among all relevant stakeholders. • Design a data layer that enables the acquisition, production, storage, and sharing of data with local communities. • Continue to reinforce the actions of the previous stage.
FROM LEARNING TO DEVELOPING
• Consider and respect the diverse rights of individuals, communities, and legal entities concerning data. • Ensure democratic governance, focusing on inclusive representation and participation, especially for marginalised communities. • Ensure the data produced and consumed is understood by all relevant stakeholders, and is consistent with the processes that create and consume the data. • Promote fair data sharing practices, establishing robust consent mechanisms and providing public data infrastructure. • Implement an optimal data layer that enables the acquisition, production, storage, and sharing of data with local communities. • Advocate for fair representation in data, acknowledging and rectifying potential misrepresentations or erasures. • Strive for equitable data ownership and value distribution in the data-driven economy. • Ensure equitable access to resources, acknowledging and addressing structural inequalities. • Facilitate national data sovereignty in alignment with international human rights covenants. • Specify and implement comprehensive data policies and management processes. • Continue to reinforce the actions of the previous stages.
FROM DEVELOPING TO MASTERING
• Develop clear ownership and stewardship structures for data, emphasising its importance as a critical asset. • Foster transparency in data practices, making crucial information about data collection and usage publicly available, including details about AI inputs and algorithms. • Enable alternative forms of data sharing/stewardship, promoting models like data commons for broader and safer data access. • Ensure democratic participation of affected communities, emphasising the importance of including all potential stakeholders in data-driven activities. • Focus on sovereign skills and infrastructure to enable local solutions and empower regulators with the necessary expertise. • Regularly update and communicate policies, standards, and processes, ensuring they are well-understood and adaptable. • Continue to reinforce the actions of the previous stages.

Appendix C: Glossary

Database: A structured collection of data, generally stored and accessed electronically (including cloud-based) that is organised to be easily accessed, managed and updated

Data Accountability: the principle that entities (be it individuals, organisations, or governments) are responsible for their actions related to data handling and processing. This includes how data is collected, stored, shared, and used, and extends to the responsible use of technologies such as artificial intelligence and machine learning.

Data Agency: capability that individuals have over their personal data. It's about people having the power to access, use, understand, and control their data.

Data Analysis : The process of cleaning, analysing and summarising data to discover useful information, inform conclusions and support decision making.

Data Analytics: The process of data analysis (compiling and analysing data) and the tools and techniques to do so, to support decision making. Could be basic counts and/or charts; descriptive (about what happened); diagnostic (about why it happened); predictive (about what will happen in future) or prescriptive analytics (about how you can do it in the best way).

Data Assets: A collection of data that holds valuable information or knowledge. This can include databases, CRM systems,
spreadsheets, mailing lists, records of transactions or bookings, collections/libraries of documents or images.

Data Collection Methods: Various ways in which data is gathered and measured to answer relevant questions in an accurate and systematic way. Methods vary according to the field of research but some examples are: observations; interviews; questionnaires and surveys; focus groups; ethnographies; oral history; case studies; experiments; randomised control trials.

Data compliance: The process by which organisations adhere to legal and regulatory requirements, as well as internal policies, for managing and protecting data. Compliance can encompass a wide range of issues, including data protection, privacy, security, and governance.

Data Infrastructure: A digital infrastructure promoting data sharing and consumption. It includes hardware (computers, phones, devices, storage and backup) and software tools which might be cloud-based

Data Fairness: concept that applies to the collection, processing, and use of data, and it emphasises equitable treatment for all individuals and groups.

Data governance: principles, practices, and processes that ensure the formal management of data assets.

Data literacy: Ability to read, understand, create, and communicate data as information.

Data Non-discrimination: principle according to which data processing, analysis, and decision-making should not result in unfair or discriminatory outcomes for certain groups or individuals based on their race, gender, age, religion, disability, or other protected characteristics

Data ownership: the legal rights and control over data. It includes determining who has the authority to access, use, dispose, modify, or share data, and who is responsible for ensuring that the data is accurate, accessible, and protected.

Data Policy: set of guidelines that governs how an organisation collects, manages, stores, and uses data. It's essentially a roadmap for how data should be handled and provides a framework for data governance within the organisation.

Data Protection: Legal control over access to and use of data held by an organisation.

Data Responsibility: ethical obligations associated with handling data. It encompasses the ways that data should be collected, stored, processed, and shared in order to respect privacy, uphold security, and ensure the rights of individuals.

Data Safety: measures and protocols put in place to protect data from loss, corruption, unauthorised access, or other types of harm

Data Security: A set of standards and technologies that protect data from intentional or accidental destruction, modification

Data sustainability: Aspects related to long-term data storage, efficient data use, and ethical and environmentally friendly data practice

Data Transparency: Principle and practice of making information available and understandable to stakeholders.

Explainability: ability to understand and interpret the decisions made by complex models of an AI/ML system understandable to humans.

Inclusion: Act of ensuring equal access to opportunities and resources for people who might otherwise be excluded or marginalised, such as those who have physical or mental disabilities, are members of racial or ethnic minorities, come from low-income backgrounds, or identify as LGBTQ+.

Open Data: Data that anyone can access, use and share. Used to bring about social, economic and environmental benefits.

Openness: Refers to the quality of being transparent, accessible, and promoting free exchange of information.

Participation: process by which individuals, communities, and organisations take active roles in decision-making, planning, and implementation of processes that directly affect them. The concept of participation emphasises the democratic principle of involving all stakeholders, especially those who are typically marginalised or excluded, to ensure that their interests and needs are considered and represented.

Right to Privacy: individual's right to keep their personal life and information confidential and free from unauthorised intrusion.

Appendix D: Printable Version of the Evaluation Grid

Name of the organisation: ***Country :*** ***Date:***

Indicators	Variables	Unaware (0 or 1)	Emerging (2 or 3)	Learning (4 or 5)	Developing (6 or 7)	Mastering (8 or 9)
Shared resources (___/45)	*Equitable access to resources*					
	Data infrastructures					
	Safety and Security					
	Data quality					
	Usability					
Community (___36)	*Participation*					
	Representation					
	Data literacy					
	Diversity and inclusiveness					
Rules (___54)	*Data sharing*					
	Transparency					
	National data sovereignty					
	Privacy					
	Responsibilities and accountability					
	Societal impact					
Governance (____54)	*Data Commons*					
	Data Justice					
	Data Rights					
	Distribution of Ownership					
	Intellectual Property Rights					
	Policies.					