# Data Governance Working Group
# A Framework Paper for GPAI's work on Data Governance

November 2020 - GPAI Montréal Summit

GPAI | THE GLOBAL PARTNERSHIP ON ARTIFICIAL INTELLIGENCE

*Please note that this report was developed by experts of the Global Partnership on Artificial Intelligence's Working Group on* the *Responsible Development, Use and Governance of AI. The report reflects the personal opinions of GPAI experts and does not necessarily reflect the views of the experts' organizations, GPAI, the OECD or their respective members.*

# Contributors

## Project lead / lead author:

**Christiane Wendehorst**

## Project Research Assistants:

**Nina Thomic and Yannic Duller**

## Project Project Steering Group:

**Alejandro Pisanty Baruch** - National Autonomous University (Mexico)
**Bertrand Monthubert** - Occitanie Data (France)
**Jeni Tennison (Working Group Co-Chair)** - Open Data Institute (UK)
**Josef Drexl** - Max Planck Institute (Germany)
**Kim McGrail** - University of British Columbia (Canada)
**Maja Bogataj Jančič (Working Group Co-Chair)** - Intellectual Property Institute (Slovenia)
**Shameek Kundu** - Standard Chartered Bank (Singapore)
**Takashi Kai** - Hitachi (Japan)
**Te Taka Keegan** - University of Waikato (New Zealand)

## With input from the wider Working Group:

**Alison Gillwald** – Research ICT Africa (South Africa / UNESCO)
**Carlo Casonato** – University of Trento (Italy)
**Carole Piovesan** – INQ Data Law (Canada)
**Christiane Wendehorst** – European Law Institute / University of Vienna (EU)
**Dewey Murdick** – Center for Security and Emerging Technology (USA)
**Hiroshi Mano** – Data Trading Alliance (Japan)
**Iris Plöger** – Federation of German Industries (Germany)
**Jeremy Achin** – DataRobot (USA)
**Matija Damjan** – University of Ljubljana (Slovenia)
**Neil Lawrence** – University of Cambridge (UK)
**Nicolas Miailhe** – The Future Society (France)
**Oreste Pollicino** – University of Bocconi (Italy)
**Paola Villerreal** – National Council for Science and Technology (Mexico)
**Paul Dalby** – Australian Institute of Machine Learning (Australia)
**P. J. Narayanan** – International Institute of Technology, Hyderabad (India)
**Teki Akuetteh Falconer** – Africa Digital Rights Hub (Ghana / UNESCO)
**V. Kamakoti** – International Institute of Technology, Madras (India)
**Yeong Zee Kin** – Infocomm Media Development Authority (Singapore)

**OECD observer: Elettra Ronchi**
**UNESCO observer: Jaco Du Toit**
**With the support of : Ed Teather,** Head of Data Governance Initiatives and International Partnerships, of the International Centre of Expertise in Montréal for the Advancement of Artificial Intelligence.

# 1. Introduction

The Global Partnership on AI ("GPAI") has been established with a **mission** to support and guide the responsible adoption of artificial intelligence (AI). It is supported in this mission by four Working Groups made up of leading international experts: (1) Responsible AI, (2) Data Governance, (3) The Future of Work, and (4) Innovation and Commercialization. According to the GPAI Terms of Reference, the **Data Governance Working Group** has a mandate to 'collate evidence, shape research, undertake applied AI projects and provide expertise on data governance, 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.' The GPAI terms of reference explicitly exclude aspects of AI and data governance related to defence and state security.

The **mandates** of the Data Governance Working Group and of the Responsible AI Working Group in particular are closely related and overlap to a certain degree. Generally speaking, the Responsible AI Working Group will be looking more into how to model AI development and how to employ which datasets, in order for AI to be shaped and to function in a responsible manner (e.g. without any undue bias). The Data Governance Working Group will therefore focus on how to collect and manage the data responsibly in the first place, in particular considering the situation of parties that are in some way or another associated with the origin and context of the data or that may otherwise be affected by use of the data (e.g. data subjects and those belonging to communities about which data is collected). The 'data perspective' and the 'algorithms perspective' are closely related, partly overlapping, and yet to some extent distinct (METI 2018; DEK 2019).

This **Framework** for GPAI's work on Data Governance has been established as the first project of the Data Governance Working Group to **set the stage** for all **future Working Group projects**. It will serve as an overview over the most relevant terms and define the understanding of the Working Group of data governance in the context of AI. This Framework paper is not meant to draw any final conclusions on AI-related data governance and is intended to be updated as the Working Group carries out deeper dives into the topics it covers.

# 2. The Role of Data in the AI Context

## 2.1. What is data?

When speaking of data as the basis of data-driven innovation and in the context of AI, we usually mean **digital data**, or data that may easily be transformed into digital data or that otherwise allows processing by machines (cf. analogous, bio, or quantum computing), while frameworks focusing on data protection/data privacy would often include also other data. Digital data consists of (i) electrical impulses, which persist on a medium or are in a state of transmission, together with (ii) context (often expressed in metadata) and (iii) semantics (such as domain tables or ontologies) which aid in its interpretation.

It is the dimension of **data as a representation of information** (ISO 2015) that counts in the data governance context. Data may have other dimensions, which are relevant in different contexts and will not be part of GPAI work on Data Governance, e.g. the GPAI Working Group on Data Governance will not be focussing on data as software (including data as AI) or on data as a representation of assets (e.g. units in cryptocurrencies).

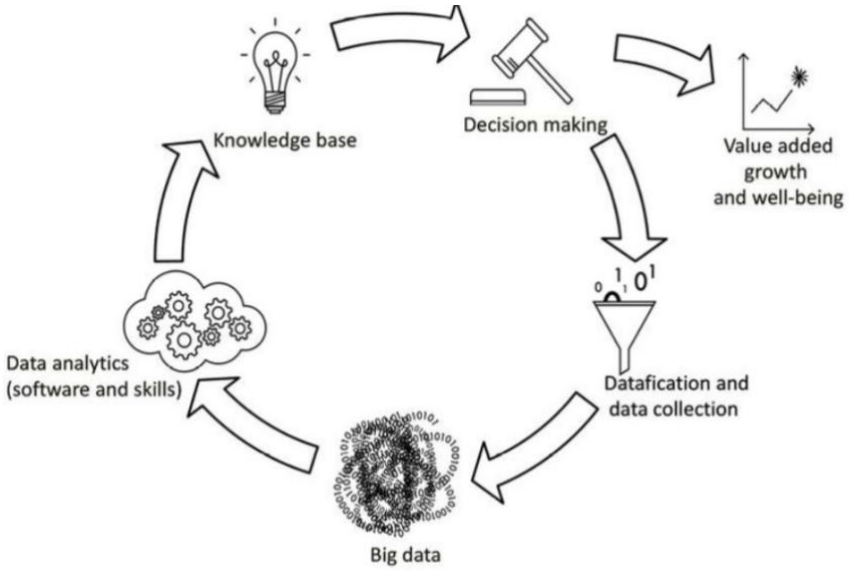


*Figure 1: Data value cycle (OECD 2015)*

Data as a representation of information is increasingly important for our societies and economies, and the data value cycle (Figure 1) has become a central part of value creation in general. Data is also at the very heart of AI, from AI's development to its deployment.

## 2.2. Data for AI development and deployment

### 2.2.1. Data for the training, validation and testing of AI

Much of what is popularly known as AI has not been (fully) programmed by human coders and is not rule-based, but has learned how to execute tasks through a process that improves performance through experience and requires large amounts of data. The use of data as **training data** as well as **validation** and **testing data** for AI has become a major reason for the increased demand for data worldwide, and the development of AI has become a major value that is created with the help of data (Figure 2).

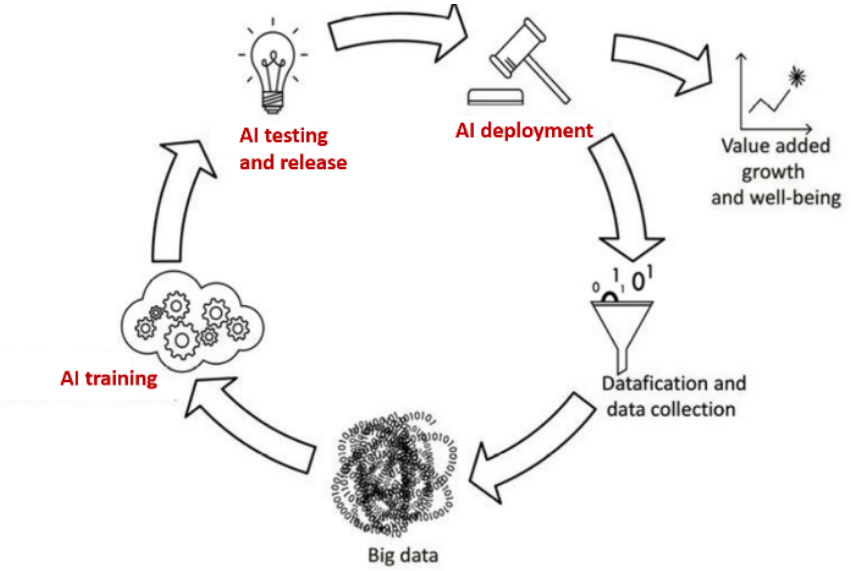


*Figure 2: Data and AI – as training and testing data (adapted from OECD 2015)*

### 2.2.2. Data as input and output of AI

Once developed and deployed, AI is also an algorithmic system. As such, it is used for processing **input data** in order to obtain particular **output data**, such as a classification, prediction or recommendation (ICO 2020) (Figure 3). This output data may immediately trigger a reaction by physical actuators (in which case we tend to speak of 'robotics'), or a non-physical reaction of some kind (in which context we often hear the term 'autonomous agents'), or merely serve as a basis for human decision-making (e.g. recommender systems). There are various different possibilities as to the division of tasks between human and machine, and different degrees of automation.

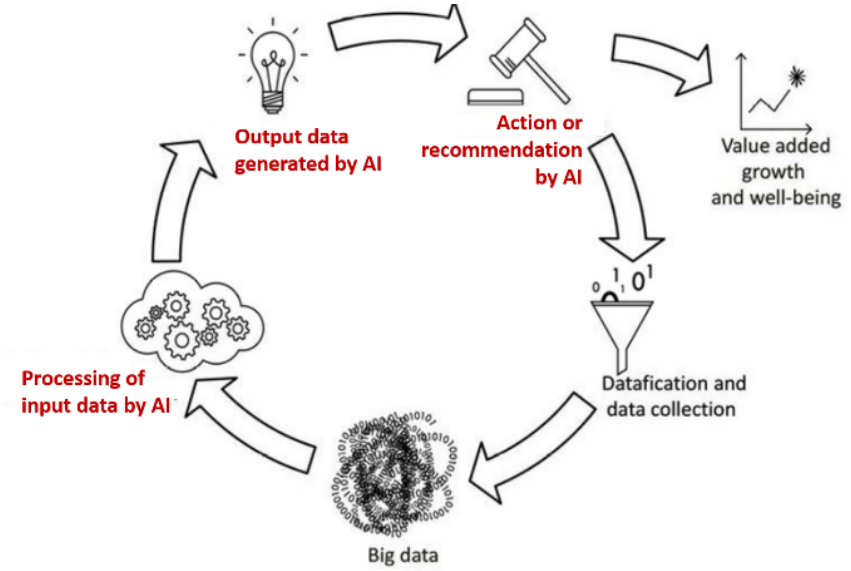


*Figure 3: Data and AI - as input and output data (adapted from OECD 2015)*

Output data may again become input or training data to the same or a different system. Both dimensions data as training and testing data as well as data as input and output data—are relevant in the data governance context. However, data governance may not mean the same for each of the two dimensions (see below 3.2).

### 2.2.3. Data specifically generated or enhanced by AI

To an increasing extent, AI is being used specifically for the **generation of (synthetic) data** that may then in turn be used, e.g. for training and testing AI (e.g. synthetic text by GPT-3). For instance, AI systems can also generate a large amount of data through 'self play', in particular in the context of reinforcement learning (see below 2.3).

Such data capture the AI's own experience in interacting with the real world either physically (e.g., robotic arms, self-driving cars on the road) or virtually (e.g., in a simulated approximate environment). Generated synthetic data and reinforcement learning are quickly becoming more and more important in AI research, development, and application.
Also, AI is highly relevant for preparing and **enhancing data** that will then be used for training or testing other AI, such as where the data that is available is not sufficiently representative and lacunae need to be filled (Rockefeller Foundation 2020).

## 2.3. Data lifecycles in the AI context

### 2.3.1. General data lifecycles

There are many different models of **general data lifecycles** (Sinaeepourfard et al 2015; Pouchard 2015). Some of them are more data-centred and visualised as a cycle, waterfall or flowchart, usually listing 5 to 8 stages, either in a linear way or with loops. A simplified, data-centred data lifecycle (e.g. Figure 4) includes steps such as the creation, collection, preparation, use, retention or preservation, sharing, re-use or deletion of data. More task-centred versions combine this with elements such as problem analysis, modelling and feedback loops.

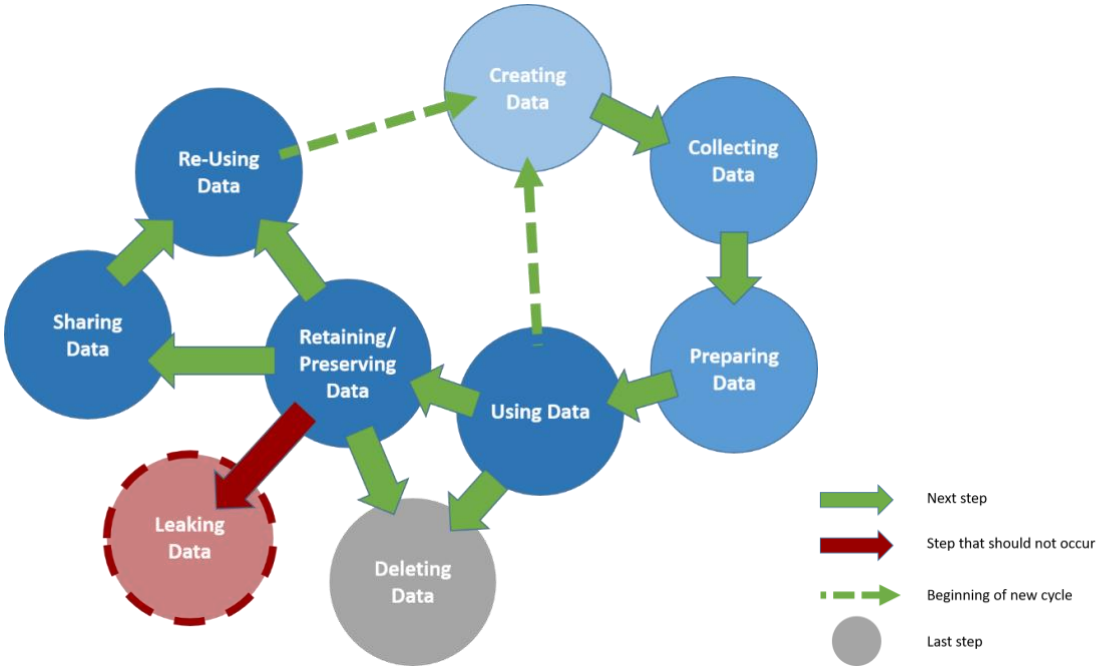


*Figure 4: Example for a data-centred model of a data lifecycle (simplified)*

Representations of data lifecycles should recognise that preparation and other processing of existing data (including, e.g. structuring, labelling, aggregation or blurring of data) may lead to the creation of new data. Models should further recognise that, at various stages, decisions (including, e.g., whether to share, preserve or delete data) need to be taken by particular actors in charge, who may of course delegate decisions to machines.

### 2.3.2 Data in the context of different types of machine learning

For our purposes, it is necessary to look more closely at what the various stages mean in an AI context, in particular collection, preparation and use of data. When doing so, it becomes apparent that there are many different pictures we see when 'zooming in' on the data lifecycle, depending on the **concrete function of data** in the AI context (see above under 2.2). More specifically, if the AI system at hand involves machine learning (ML), much depends on what **type of ML** is being applied.

**Supervised** learning is about **inferring a function from labelled input-output data pairs**. This function should allow the algorithm to correctly determine, inter alia, the class labels and decision trees for unseen instances (e.g. in order to differentiate between cats and dogs, or between static and moving objects). In terms of data governance, much depends on the choice (and, if necessary, generation) of the training data pairs, on the labelling of these data pairs, on the modelling and learning itself, and on correction of sub-optimal outcomes in the re-training and validation phase (Figure 5). At each of these stages, errors, bias or other undesired events may occur.

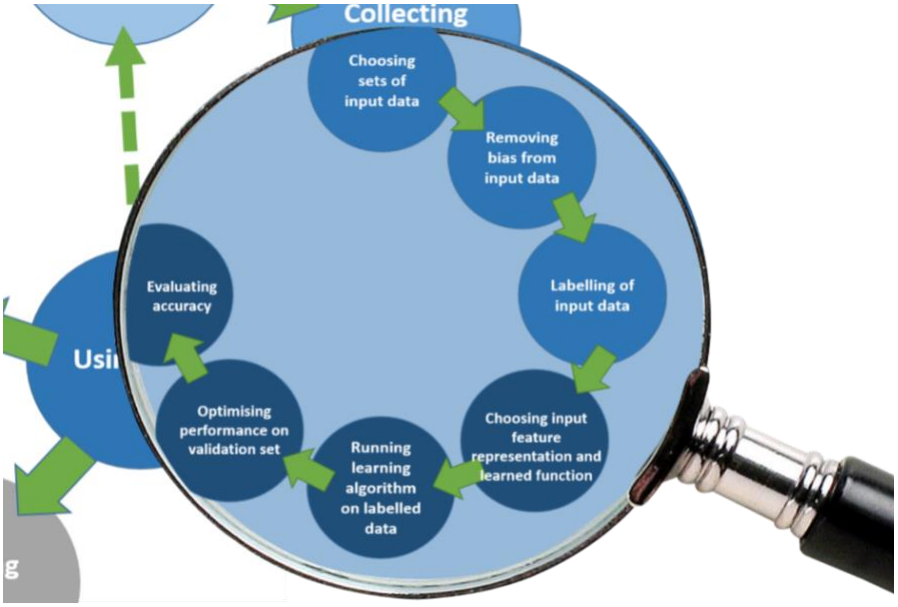


*Figure 5: Refinement and use of data illustrated for an example of supervised learning (simplified)*

**Unsupervised** learning looks for **previously undetected patterns in a data set with no pre-existing labels** (e.g. in order to classify different classes of consumers in a large customer database). The goal could be, e.g. to group or segment datasets with shared attributes (clustering) in order to extrapolate algorithmic relationships between them (association). Unsupervised learning normally uses large and unstructured data sets. Patterns not (sufficiently) present in the training data sets cannot be detected, so it is essential that training data is inclusive, and bias should be sought and adjusted for in the analysis (e.g. by using statistical tools). While the quantity and granularity of training data is very important for ensuring a good learning outcome, much less attention may be paid in terms of data governance to adding the 'wrong' data sets as the algorithm will ideally ignore the irrelevant ones. Results must be treated with utmost caution and must be carefully validated as they reflect correlations rather than causal relationships.

**Reinforcement** learning is about finding the **best possible path of action in a specific situation in order to maximise cumulative reward**, which in turn is connected with the degree of achievement of a pre-defined goal. This differs from supervised learning in not inferring a function from labelled input-output data pairs, but from the level of reward received after taking a particular path (trial-and-error). Recent developments in reinforcement learning can express in written form the heuristics or rules that should be followed to maximise cumulative rewards for the particular training example. Reinforced learning relies on data to a much lesser extent than supervised or unsupervised learning. However, someone needs to define goal-achievement and how to score different outcomes, which may be straightforward (e.g. winning a chess game) or rely on the accuracy of pre-existing validation data sets (e.g. for evaluating the validity of different predictions).

Other distinctions that are relevant for data governance include the distinction between **centralised and federated learning**, depending on whether data required for AI development is moved to the learning algorithms, or whether, conversely, the learning algorithms move to the data. The latter model allows data to be held in a decentralised way with less information being disclosed to the developers (McMahan and Ramage 2017).

For each of these ML methods, a range of different sub-methods exist, and the methods are often not applied in their pure form, but are **combined** (e.g. Visual Question Answering combines computer vision, natural language processing, deep learning and reasoning to create a technology that can answer open questions about new images). In a broader and more technologically neutral sense, AI may not even rely on ML at all, but on **complex rule-based coding**, resulting in algorithms suitable for fulfilling very sophisticated tasks. Even in the latter case, however, data play an important role in the development phase: rule-based systems also need to be tested and validated on the basis of pre-existing data sets in order to check whether processing of input data leads to output data that is known to be correct.

# 3. Why Data Governance for AI Matters

Data governance is not an end in itself – it should help us achieve what we consider as desirable, and avoid what we consider as undesirable. With the enhanced roll-out of AI there is an increasing number of case studies that demonstrate what can go wrong without good data governance, and how AI can be used for the benefit of us all where good data governance is observed.

## 3.1. Case studies

### Case Study No. 1: AI recruitment tools – using the wrong data for the AI at hand

In many sectors women are structurally underrepresented compared to men; this is especially true for managing or other well-paid positions. Where companies automatize their hiring process, the existing bias against women may also be reflected in the AI based hiring tool. (Reuters 2018).

Recruitment algorithms usually assign scores to applicants (e.g. one to five, one being the worst, five being the best). Women are particularly disadvantaged if such scores do not reflect their abilities. Even though such unfavourable scores can also result from bias within the design of the algorithm itself, in the past, the problem seemed to stem even more from the wrong data sets being used. For example, if algorithms were trained to review applicants by observing patterns in resumes submitted to the company in the past and the majority of successful applications came from men, the algorithm will teach itself that male applicants are to be preferred over female applicants. However, such technologies could also be quite promising to reduce bias in traditional hiring decisions, as they can sometimes be more objective than HR officers (Harvard Business Review 2019).

This use case provides a well-established example of how the use of biased data sets can lead to discriminatory outputs by AI. Good data governance needs to ensure that the data used is appropriate for the intended purpose.

### Case Study No. 2: COVID-19 research related to public health – lack of access to data required for AI

In the course of the COVID-19 pandemic, medical research is vital to overcome global challenges. In particular, there are research projects aimed at improving our understanding of COVID-19 by reviewing scientific literature and projects focusing on the development of tools to effectively combat the spread of COVID-19 with the help of medical or other data from individuals. Even though the latter might have a more direct and ad hoc influence on decisions of health authorities, they both show difficulties related to the availability and access to data.

The lack of access to COVID-19-related literature results partly from business models of major publishing houses that limit public access entirely or at least access in machine-readable format, meaning an approach to data governance that significantly limits the use of AI in a way that hugely benefits our societies. Pressure by the WHO, individuals, and governments resulted in a commitment for publishers to provide machine-readable access to COVID-19 related publications. The resulting COVID-19 Open Research Dataset (CORD-19) consists of nearly 200,000 entries, including thousands of articles that serve as a basis for data mining exploration using ML techniques (OECD 2020, Semantic Scholar 2020). The machine-readability of data available via CORD-19 is currently being tested, e.g. with a competition by Kaggle (Kaggle 2020) and by ongoing research.

For research on the way the virus spreads and affects the human body, medical data (e.g. also on comorbidities of a COVID-19 infection), social data (e.g. affiliation to a certain age group) or mobility data can play a vital role. For example, a hospital in France is developing a decision support tool consisting of a map of the areas where the virus is likely to reappear in the surroundings, which can help health authorities in taking preventive measures to limit the spread of the pandemic. However, the project team does not have sufficient data at their disposal. Such data exists but is quite difficult to access, e.g. due to privacy considerations, but also due to logistical barriers (data holders expect revenue for providing access to data, different procedures to gain data access, lack of interoperability). Effective governance measures, such as access to data within secure data spaces, managed by trusted parties, and under clear and transparent conditions that include appropriate safeguards for the legitimate interests of all stakeholders involved, would be vital to make important scientific progress.

### Case Study No. 3: Financial inclusion – ensuring responsible data use

Despite Despite significant progress in making financial services more accessible (e.g. through the development of banking apps and new payment methods), around 1.7 billion adults, often in developing economies, still do not have a bank account at all (World Bank 2018). However, this part of the world's population could benefit immensely from access to financial services (e.g. for the development of SMEs), and so can banking institutions, as the unbanked population opens up a massive market for growth (Tata Consultancy Services 2019).

AI can play a huge role in expanding financial inclusion. It allows financial institutions to manage the risk and cost of serving this segment more effectively. Alternative data and algorithms can make it feasible to provide insurance or lending to customers that were previously seen as unviable or too risky (CFI 2019). It is important to note that such alternative data sources, however, can raise important issues, such as consent management, as consumers would have to agree to very private data (e.g. from social media) being exposed to financial institutions in order for them to receive loans (World Bank and CGAP 2018). Nevertheless, the management of customer characteristics and financial crime considerations, can be carried out much easier with support of AI and access to alternative data. Especially SMEs can profit from better accessibility to credit, which could in turn lead to new employment opportunities and economic growth (MINT 2020). Even those who already have access to a bank account can start benefiting from new services.

However, making this happen requires good data governance in particular regarding the responsible use of alternative data (e.g. consent management, making sure the data used is accurate, preventing use of inappropriate types of data or inferences such as relating to sexual orientation, preventing use for purposes that are inconsistent with the initial purpose).

## 3.2. Aspects of data governance

Good data governance may mean different things with regard to the use of data as training and testing data for AI development with regard to the use of data as input and output data where AI is deployed, and with regard to wider data ecosystems (Figure 6)). In each of these cases good data governance should be **risk-based** as the need for data governance measures increases with the potential impact an activity may have on others, including on society and economy at large.

It is important to understand that **governance of training and testing data** (above 2.2.1 and 2.3.2) involves an **'instrumental' perspective**, i.e. as AI services and products are brought to the market, the type and scope of the datasets must be designed in a way that leads to the functions and performances that are intended. What counts from an instrumental perspective is that the resulting AI is trustworthy and responsible, while there are only few standards that would apply to the data per se and without regard to their effect on the resulting AI. For instance, accuracy of data is not important per se, and may even be detrimental: data that accurately reflects personnel decisions in a company over the past decades may be excellent for ex post-analysis (e.g. with a view to detect discrimination), but unsuitable for training human resources software for future decision making (exactly because of the bias in the data). Inclusiveness and diversity are generally very important (Rockefeller Foundation 2020; HLEG AI 2019; Diversity.AI 2017), and exclusion or marginalisation of particular groups (e.g. based on their gender, cf. also use case no. 1) is a major problem and may amplify existing social inequalities and sustaining patterns of disadvantage (IFO 2020), but only where the AI that is developed will include application with regard to those groups. It may even be the case that, in order to achieve fairness, handling of training data is forced to 'discriminate': one reliable way to avoid discriminative effects in recidivism prediction software may be to sort the data sets by highly sensitive criteria (such as colour) and train the AI separately. Needless to say, the governance of training and testing data involves much more than the instrumental perspective and must make sure, in particular, that no rights of third parties are infringed by the use of the data ('**data origin perspective**'). This includes transparency in the value chain on how AI was trained and in particular where the data sets used stem from (e.g. that they were provided from a trustworthy source and that data was not misappropriated).

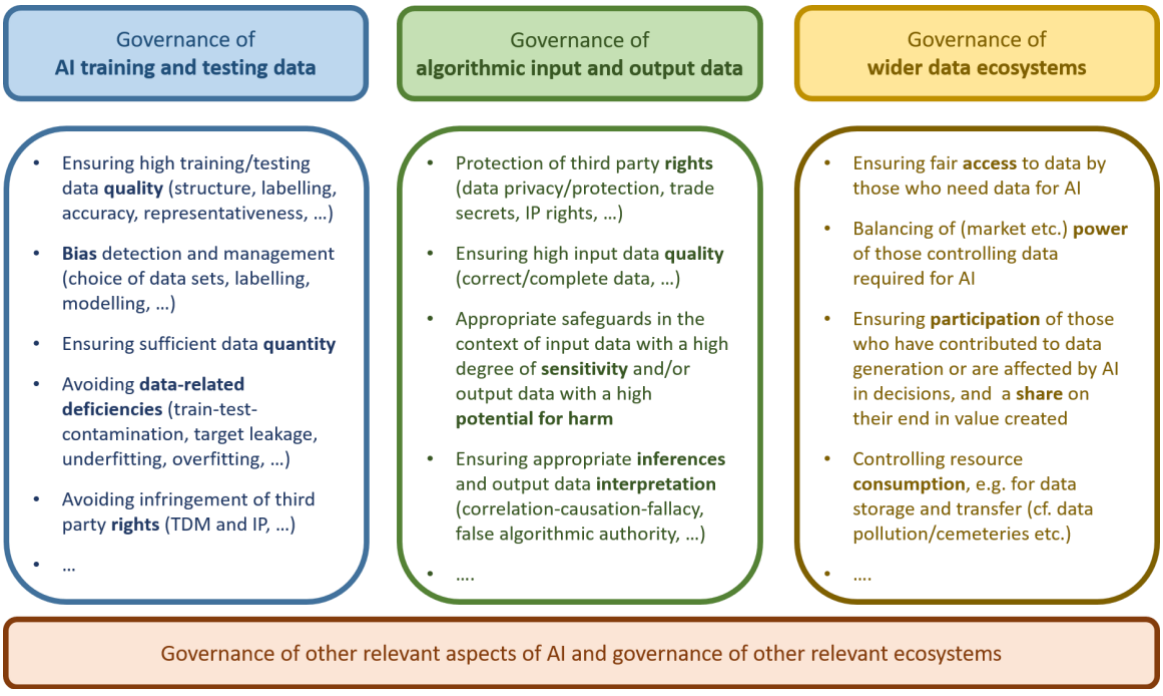


*Figure 6: The need for data governance in the AI context*

The **governance of input and output data** focuses, in particular, on the rights and legitimate interests of parties that have something to do with the origin of input data or that may be affected by output data ('**responsible use perspective**'). This includes rights based on data privacy/protection law, IP law or other bodies of the law (for details see 4.3) or rights and legitimate interests not to be subjected to unreasonable or unfair automated decision-making. It is important to understand that governance of input and output data differs from governance of training and testing data. Sensitivity of input and output data is a major issue: an individual may care little when their data is used merely for training AI that will calculate other people's credit scores, but will care very much when their data is used as input data for calculating their own credit score. Accuracy and completeness of input and output data are highly relevant per se, whereas bias in input data often is not: a gender bias in the data used for training credit scoring AI matters, but any such imbalance in a group of customers seeking credit is largely irrelevant. To an increasing extent, there are risks associated with inappropriate inferences and output data interpretation, which largely stem from (unintended or deliberate) ignorance of the validity of output data on the part of those who base their decisions on them.

Finally, **governance of wider data ecosystems** becomes ever more relevant, and even more so as the development and deployment of AI requires data. This type of governance may look at the location and means of data storage, as well as on the way data is accessed and shared, or, in fact, deleted, as more and more companies are struggling with too large amounts of data. It may also look at bigger societal, economic and environmental effects. Governance of data ecosystems must address (lack of) access to data on the part of those who need data, increasing influence and market power on the part of those who control data, fair participation on the part of those who contribute to data generation, and consumption of energy or other resources for data collection, storage, and transfer. Good data governance of wider ecosystems is able create a basis for an environment that builds **trust in AI that is trustworthy**, and in other trustworthy data-driven technologies, among society and thus to facilitate the uptake of this new technology (EC 2020; Montréal 2018). This in turn will encourage the **sharing of data** for the benefit of innovation and growth (WEF 2020; ERC 2014).

Finally, it is important to acknowledge that data governance does not come as a task isolated from other governance tasks in the context of AI, nor from the **governance of ecosystems that are not data-specific**. Anything that can be analysed as an issue of data governance might often as well be analysed as an issue within a different, not necessarily data-specific context (e.g. bias in training data and resulting deficiencies of the AI may be discussed in the context of data governance, or of AI design, or of discrimination in general as a major societal problem). It is essential for good data governance to keep other governance frameworks in mind and to try to achieve a high degree of consistency.

## 3.3. Data governance – whose task and at what level?

Governance is a task not just for one class of stakeholders. Rather, we must strive towards **multi-stakeholder governance** (e.g. OECD 2019; CoE 2018; ODC 2015). There is data governance from a State actor perspective and from the perspective of private parties (METI 2020). **Policymakers** – at international, national, regional and local levels – would be looking at regulation, but also at a host of other governance tools, including education and information campaigns (with a view to improving data awareness and data skills), provision of data infrastructures (such as data spaces or data trust schemes), promotion of certain economies, tax benefits, etc. For **data holders** (private or public), data governance is mainly data lifecycle management, a complex task involving aspects of corporate asset management, choice of business models, corporate ethics and corporate social responsibility. Increasingly, data governance is also a task for **communities**, such as indigenous peoples, communities or organisations of the civil society, who might also be actively shaping policies as governments have committed to take their views into account. It is also a task for **private-public consortia** which can work on some projects involving data from each partner of the consortium, usually in order to achieve some project of public interest.

Data governance regimes can also be of very different scope. There is a discussion on **sectoral** data governance regimes, which has the advantage of more targeted rules that allow a better balancing of interests of the concrete group of stakeholders. Pharmaceutical research, for instance, concerns different stakeholders than use of data in agriculture with implications for the environment and the climate. Yet we also need to think in terms of **cross-sectoral** data governance since the different sectors are not completely isolated (EC 2020, OECD 2019, ECHAlliance 2020). For instance, traffic data generated for the purpose of traffic regulation and safety purposes may also be used for other purposes, such as environmental protection.

Data governance can also occur at **national or supranational or international level**. International data governance strongly links with the UN Sustainable Development Goals. From an ethical perspective, there is also a justice argument that should require international data governance systems to guarantee that not only some countries (or their firms) get access and benefit from the exploitation of data, while others only provide access to the data available in their borders without benefiting from their commercialization.

## 3.4. Ethical and other principles of Data Governance

### 3.4.1. Principled approaches to data governance

There are many different approaches to data governance, ranging from purely taxonomic frameworks to identification of strategic priority areas, to guidance documents for compliance with data protection rules worldwide, to legislative measures that facilitate the free flow of data, or very practical checklists to be used, e.g. by particular departments in an organisation. What is arguably the majority of data governance frameworks developed so far have taken an **ethical and principled approach**, trying to express in a more prescriptive/normative manner what should be the guiding considerations for actors who have to make decisions at various points in the data lifecycle. They include in particular, but not exclusively

- policies that should guide any **decision** to be made about data throughout the data lifecycle;
- requirements to be met by any concrete data **activities**;
- standards for data preparation and storage to create sustainable **value**; and
- data **sharing** with a view to the right balance between opening data up and closing it down.

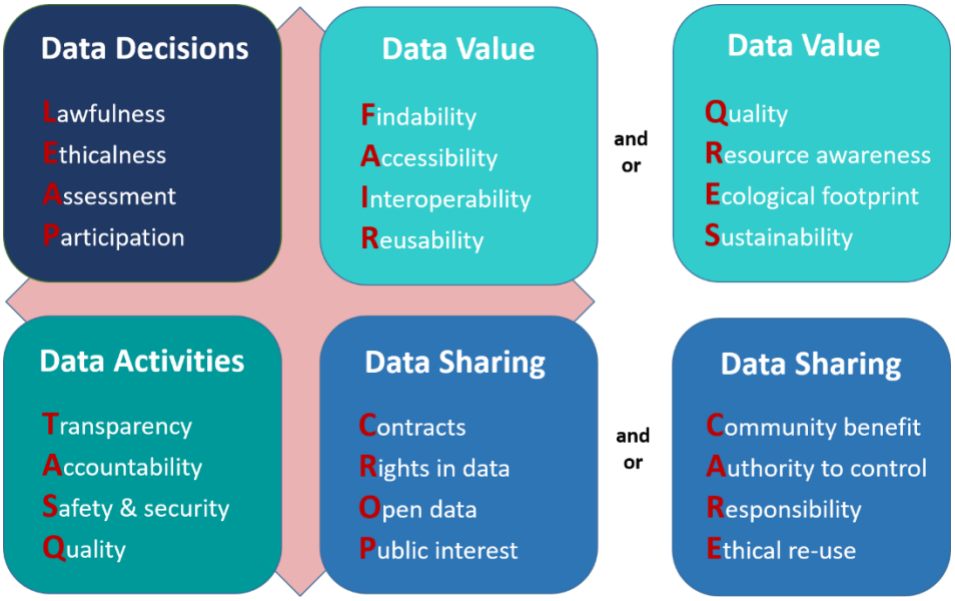


*Figure 7: Systematisation of data governance principles*

Principles for responsible AI is a subject which has given rise to important texts and drafts (such as OECD 2019; HLEG AI 2019; Montréal 2018, please also see the Annex for other frameworks). Attempts to issue the equivalent for data have been undertaken, e.g. by Denmark (EGDE 2018), the UK (UKDS 2018) and Germany (DEK 2019), and are underway in France (Occitanie 2020). They are also undertaken by private companies, such as in the IT and consultancy sector (e.g. Accenture 2016). Some frameworks specifically address the use of data in the context of AI (e.g. OHCHR 2020).

While the level of abstraction and the corresponding number and exact denomination of principles identified varies, usually ranging somewhere between 4 and 12, there is far-reaching consensus as to their broad content. The overview in Figure 7 systematises the principles to be found in data governance frameworks worldwide, arranging them in groups and following the international habit of creating acronyms. Some of these acronyms are already widely recognised, such as the FAIR Principles (Wilkinson et al 2016; GOFAIR 2019).

### 3.4.2. Consensus and debate

There is normally broad consensus that data governance, and relevant governance decisions, must be lawful and ethical, that they must be subject to careful assessment (including wider impacts) and seek participation of all relevant stakeholders (**LEAP**). 'Ethical' is potentially a very encompassing notion, and it may even be possible to subsume everything that comes as 'data governance' under 'data ethics'. Data ethics comprises very fundamental principles, such as non-malevolence ('Do not harm'), benevolence ('Do good'), equal liberty ('Respect the freedom of others') and fair distribution ('Give everyone their share'). It also comprises more concrete standards, such as (per the GPAI mandate) human rights, inclusion, diversity, innovation, economic growth, environmental protection, and societal benefit, as enshrined in the UN Sustainable Development Goals. What is considered ethical may depend on the cultural framework within which players are operating, again from the very local to the global.

There also seems to be broad 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 (**TASQ**) are of utmost relevance for any kind of data activities. When it comes to creating data value and enhancing access to as well as sharing and re-use of data, it is more concretely the **FAIR Principles**, calling for findability, accessibility, interoperability and reusability, which have gained worldwide recognition (Figure 8).

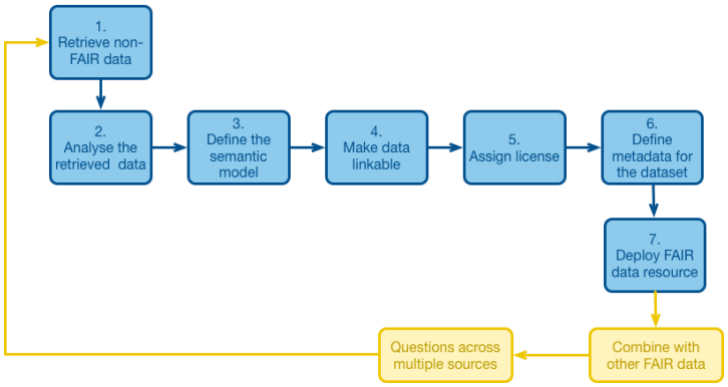


*Figure 8: FAIRification process (GOFAIR 2019)*

Of late, the focus of the principles that should be guiding the sharing of data have increasingly become the subject of discussion. In addition to the FAIR Principles, stress is often put on the existence of, and the need to enhance, different cross-sectoral frameworks for data sharing and corresponding access and control mechanisms (OECD 2019; ELI 2020, EC 2020), such as contractual agreements, portability and similar rights in data, open data and more restricted arrangements, most of them for the public interest (**CROP**). However, it is also pointed out that FAIR and CROP are benefitting in a rather one-sided manner particular players and regions of the world (e.g. with an uneven distribution especially in the Global South), potentially resulting in 'data colonialism' (MEIT 2019). This is why also a **CARE** regime has been argued for (GIDA 2018), stressing more 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 (see also USIDSN 2020). More generally, there is increasing support for involving individuals, communities and peoples directly in setting rules around data collection, use and interpretation, understanding that use of data is evolving rapidly and has a very strong normative, values-based component (e.g. AI4D 2020).

Even more recently, there is growing concern about digital consumption in terms of energy and other resources, calling for '**digital sobriety**' (Ferreboeuf 2019; Itten 2020). This could mean a paradigm shift from an attitude that believed in data maximisation – hoping that more data would lead to better technologies and better decisions, including technologies and decisions that foster sustainable development – to an attitude that stresses quality, resource and wider ecological footprint awareness as well as sustainability (**QRES**) in the first place.

# 4. Parameters for Data Governance

Besides the question of the particular function of data within the AI context, there are a number of further parameters that have an impact on data governance, including categories of data, roles and actors in data ecosystems and rights with regard to data.

## 4.1. Categories of data

### 4.1.1. Technical categories

Data can be classified into different technical categories of data according to a number of different criteria, such as the division between **unstructured** (raw) data and **structured** or more **refined** data, or according to different data **types** (e.g., binary, nominal, ordinal, metric and textual data) or **functions** (e.g., imagery, video, sound, streaming/real-time data, and text). There are some data governance approaches that are more or less appropriate for different categories, and some types of data are more relevant in an AI context (e.g., real-time data may need a different approach to bulk access data; AI-based pattern recognition is particularly useful over unstructured data and imagery).

**Metadata** (as a subcategory of **reference data**) is data that provides information about other data, such as descriptive, structural, administrative, reference and statistical metadata (CoE 2020). Metadata is of utmost importance for data governance in general, including for implementing FAIR Principles (see 3.4) and for data provenance and lineage governance that is, amongst others, required for data rights management (see 4.3). Metadata and provenance, describing the data generation process and thus who/what is and is not in the data, are also critical for understanding bias and thus implementing other aspects of data governance.

We can also distinguish between so called 'real' data that represent information about the 'real world' and that has been obtained, or might theoretically be verified, by direct measurement, and **synthetic data**, i.e. artificially created substitutes for real world phenomena (e.g. through simulation). The latter may serve a range of different purposes and can, in particular, be a more privacy-friendly or more affordable alternative to real data or ensure better representativeness or other desired features in the context of AI.

A lot of buzz has emerged around the term '**Big Data'** and its counterpart '**Small Data**'. While various definitions exist and it has become a habit to define Big Data by varying numbers of "V"s (e.g. Gartner), the main message is that the exponential increase in storage space and computing power fundamentally changes how data is used and managed. Big Data and Small Data may pose different challenges for data governance, but data governance should address both.

### 4.1.2. Categories related with actors involved

Some Some important divisions for data governance purposes are based on the (assumed) **'sensitivity'** of data. A central category is that of **'personal data',** as contrasted with 'non-personal data', which is used to define the scope of application of data privacy/data protection laws (see 4.3.1). Different laws in different jurisdictions have different definitions of personal data, including definitions of 'pseudonymised' and 'anonymised' data, and their legal status. Frequently, special sub-categories of personal data are created (e.g. health data, biometrical data). Among what is normally called 'non-personal data', there is data that refers to an identifiable business or other legal entity (**'legal entity data'**), and data that refers neither to a natural person nor to a legal entity. Generally speaking, the former is more sensitive than the latter, but even data of the latter type can be 'sensitive' in the sense that disclosure might cause harm, including to the environment (e.g. data about the locations of endangered animals, ODI 2019), business interests (e.g. commercially sensitive data), and to national security (e.g. military secrets). Increasingly, the paradigm of bi-lateral relations between a person or entity to whom data refers and a controller of data is being called into question. Data is multi-relational in the sense that a decision taken by one person with regard to 'their' data may affect others (e.g. by allowing inferences about them). Equally, there is growing recognition of data sovereignty rights held by indigenous peoples and of other group rights over data.

Another important division that looks at the origin of data (Abrams 2014; WEF 2014; OECD 2019**)** is that between **provided data** (i.e. data actively supplied to the controller of data by the person to whom the data refers or from whom the data otherwise stems); **observed data** (i.e. data recorded by the controller through observing another person or their activities); **derived data** (i.e. data generated by the controller by mechanical processing of other data, which may in turn be supplied or observed); and **inferred data** (i.e. data generated by the controller from other data, which may in turn be provided, observed or derived, with the help of probabilistic assumptions, e.g. credit scores). Where data does not qualify as provided data because it was supplied by a third party it is usually called **supplied data**. These categories are used to justify, e.g. differences with regard to data rights, such as a frequent limitation of data portability rights to provided data (see also 4.3.2 and 4.3.3**)**.

Yet another distinction looks more at the way data is kept close or shared with others, which often correlates with the sensitivity of data. Data access constraints exist on a spectrum, which ranges **from closed to shared to open** (cf. the ODI data spectrum).

Another distinction can be made between data the use of which may result in an infringement of certain forms of **legal protection**, such as IP rights, trade secrets protection or investment-related protection, on the one hand, and data that can be freely used legally, on the other hand (for more details see 4.3).

## 4.2. Data ecosystems

### 4.2.1. Actors in data ecosystems

Data governance has to take into account the rights and legitimate interests of different actors in data ecosystems (Figure 9). The central figure among the actors involved is the **controller** (also: **holder** or, depending on the context, 'steward') of data, who decides about the purposes and means of their processing. 'Control' is a factual notion and does not necessarily imply that the person exercising control has a right to do so. Control may be exercised jointly with other **co-controllers** (e.g., in a data pooling arrangement). **Data processors** act as service providers that process data on a controller's behalf.

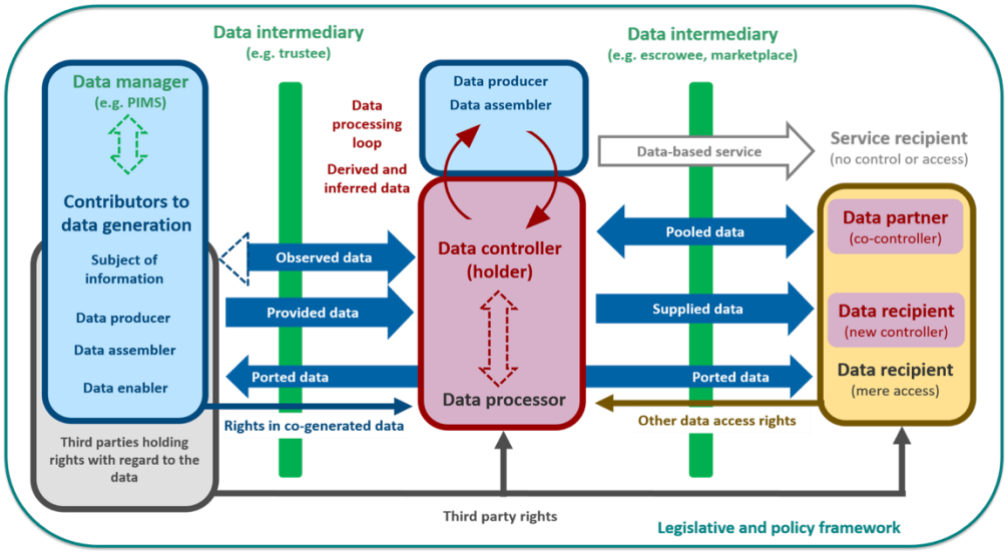


*Figure 9: Actors in a traditional data ecosystem*

Various different parties can contribute to the generation of data (OECD 2019), e.g. by being the individual or legal entity that is the **subject of the information** recorded in the data (or, that owns or operates the subject of the information, such as where data refers to land the person owns). Another way of contributing to the generation of data is by being a **data producer**, i.e. recording information that had previously not been recorded by one's activity, such as by driving a connected car (but cf. the controversy over whether the data are produced by the drivers or by the manufacturers). Note that a controller of data that engages in processing operations is, with regard to the data they derive or infer, also a data producer ('data processing loop'). Other parties do not produce new data but act as a '**data assembler**' (also: 'aggregator'), such as by creating a database. There are also a range of '**data enablers**' that contribute in more remote roles (e.g. the producer of a device that generates data). All of these actors, plus further third parties that may be affected in various ways, may have rights against controllers of data.

Where a (first) controller of data supplies the data to third parties, the latter are usually referred to as **'data recipients'** (depending on the context also 'data re-users'). In addition to the parties mentioned there is an increasing number of different types of **data intermediaries** as data sharing service providers, such as data trustees, data escrows, or data marketplace providers. They facilitate the transactions between the different actors, such as by acting as a trusted third party (EC 2020).

The roll-out of AI systems also means that decisions with regard to data are often not taken directly by human actors (who may be acting on behalf of other natural persons or legal entities), but that instead decisions are outsourced to machines. It is still, at least for the time being, human actors that have designed the machines and have set them in motion and that have to take responsibility, but it may mean a shift from 'data governance' to **'data governance-by-design'**.

### 4.2.2. Data-driven business models

The economic impact of data is rapidly growing and many business models are built on data (EC 2020). First of all, data can be used by the data holder for **developing innovative products and services** of any kind, including any AI, which can then be used commercially and marketed by the data holder. In a similar vein, data holders can use knowledge derived from data for improving any product or service, or **improving their business operations** in general (e.g. by analysing demand by their customers). However, it is equally possible that data is used for continuously **fuelling data-based services** (e.g. targeted advertising, predictive maintenance) provided commercially by the data holder to service recipients. Both models are being used by big **digital platforms** that take advantage of the network effects of data: the more users they have, the more insights they can gain from data about those users (often using AI), the better the service they can offer, and the more users they can attract. Enabling access to this (often sensitive and personal) data is one tool competition authorities are exploring to increase competition in digital markets (OECD 2020; Furman 2019).

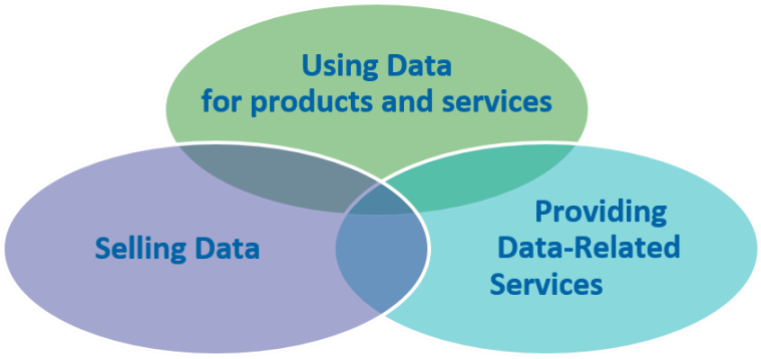


*Figure 10: Data-driven business models*

Businesses may also make money by **selling data**. This may occur by businesses not originally in the 'data sector' (e.g., some manufacturer of machines does not use the machine-generated data itself, but finds someone who is prepared to buy them for money). However, it may equally occur by professional **data brokers**, whose business it is to trade in data and add value to it by locating, standardising, aggregating, combining and/or deriving data from the data they source. Serious data governance issues arise as data passes through these data brokers. In particular, it becomes important to ensure that these brokers adhere to expected standards, and for the eventual users of that data to access information about its provenance, the methods, ethics and legality of its collection, and the techniques used to derive data.

Last but not least, there is an ever broader range of **services provided with regard to data**. These services can be services for data **processing** in the widest sense, including, for instance, the collection and recording of data (e.g. data scraping), storage or retrieval of data (e.g. cloud space provision), analysis of data (e.g. data analytics services) or the organization, structuring, alteration or combination of data (e.g. data platform services). They can equally be data **intermediary** services, such as the services provided by data trustees, data escrowees, or data marketplaces (that facilitate matchmaking rather than act as data brokers themselves) (EC 2020).

## 4.3. Rights with regard to Data

Data governance has to consider and respect a range of different rights which natural or legal persons, peoples or communities may have with regard to that data. Such rights may be of a very different nature and origin, and they are often not data-specific (e.g. there is a right not to be discriminated against in the workplace on grounds of gender, irrespective of whether such discrimination has anything to do with data). However, there is also a growing body of data-specific rights.

### 4.3.1 Personality rights

Individuals may have personality rights with regard to data, notably personal data referring to them, which is recognised by **data privacy/data protection** laws. There is a spectrum of different conceptual frameworks, ranging from more property-oriented models (which accept, e.g. that an individual markets their personal data) to privacy-oriented models (which put the stress on keeping potentially sensitive information secret) to human rights-oriented models (which see informational self-determination as a human right, comparable to life or bodily integrity, and would usually oppose any marketing of personal data by an individual; OHCHR 2018). Personality rights hugely impact the use of AI, in particular in the deployment phase. The scope of data privacy/data protection regimes varies from jurisdiction to jurisdiction. An underlying tension exists between those data protection regimes that are based on the idea of **data minimisation**, and the need for more data in order to develop and train AI.

### 4.3.2. Intellectual property (IP) and related rights

Data may also be protected by certain rights of a largely economic nature (Drexl 2017). However, the relationship of **IP protection** and data can be very complex. While patent law provides for an exclusive right of use and economic exploitation of technical information (data), copyright law only protects the creative elements of a protected work. Accordingly, the information (data) contained in a given work (e.g. a scientific article), is not 'owned' by the copyright holder. Yet copyright can create impediments to access and use of information in a digital context. For instance, digital text and data mining may technically require or involve a more comprehensive copying of a dataset including copyright works, thereby resulting in a copying of the creative elements of such works. Similarly, sui generis **database rights,** as available especially in the EU, only protect the database and not the individual information contained in it. However, potential sui generis database rights, as well as the copyright in creative databases, could result in restrictions on access to information. Copyright and sui generis database protection massively affects the availability of data for AI, and the exceptions and limitations in an AI context, such as for text and data mining (TDM) (Japan 2018 with English summary here; EU 2019), are currently still underdeveloped in many regions. One solution could be to support the use of open-source frameworks as they can be a tool to decrease impediments and allow for access to data without violating IP law (UNESCO 2019).

Alongside intellectual property law, even **unfair competition law** could provide protection, such as against parasitic copying, which often has similar effects in practice. Depending on the content of data, their economic value and on whether they are kept secret by their holder, data may also be protected under **trade secrets law**. The exact extent to which data is covered by all these regimes is not yet wholly settled and varies from jurisdiction to jurisdiction.

### 4.3.3. Rights in co-generated data (data ownership/sovereignty rights)

For data that is not subject to a specific protective regime such as IP law, there have been debates as to whether general **'data ownership'** (or a 'data producer right' etc.) should be recognised. While it is very common to speak of the 'data owner' in the sense of a rightful holder of data, or of someone who has initially generated data or should otherwise legitimately exercise **'data sovereignty'**, it has turned out to be very difficult and not advisable to recognise general ownership rights—understood in the traditional sense of exclusive property rights with full third party effect—in data (MPI 2016).

Recently, a global trend seems to move into the direction of **specific 'data rights'**, notably rights in co-generated data (ALI & ELI 2018; DEK 2019; EC 2020), which includes personal, non-personal and group data, and of which a data subject's rights under data privacy/data protection law are only a particularly important sub-category. Data rights are legally protected interests that arise from the very nature of data as a non-rivalrous resource, which may be used by many different parties at the same time. Rights of this nature serve functions similar to those fulfilled by property with regard to traditional rivalrous assets. The most important basic data rights are (ALI & ELI 2018): **access** to or **portability** of data, **desistance** from the use of data**, correction** of data and **economic share** in profits derived from data.

Data rights in co-generated data take account of the fact that data is usually generated by different contributions from various parties, e.g. by being the subject of the information, by performing an activity by which the data were generated, or by having rights in a product or service that has contributed to the generation of data (see above 4.2). Co-generation is not just a matter of Yes or No, but rather a matter of degree. Having contributed to the generation of the data can justify the recognition of a data right against the controller of the data, but is only one out of several factors that have to be considered, these factors including the scope and nature of the party's contribution or the legitimate interests of other parties (Figure 11).

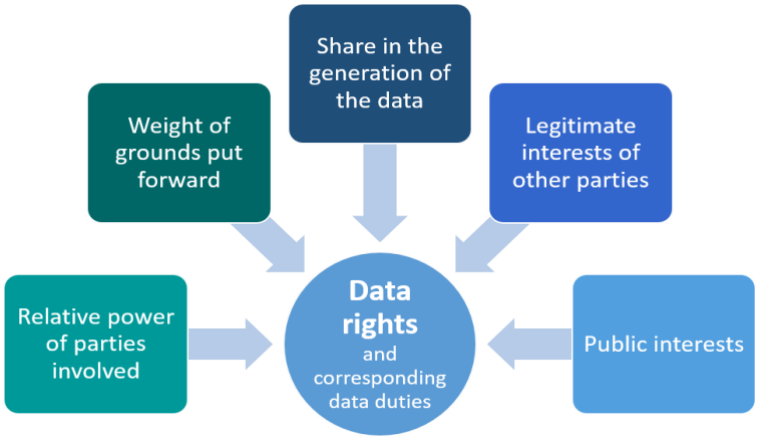


*Figure 11: Factors determining data rights in co-generated data (ELI 2020)*

Data Data rights in co-generated data are often individual rights, but they can also be asserted by **communities** that have contributed to the generation of data in some meaningful way (e.g. regions of the world may have collective data rights to prevent 'data colonialism') (MEIT India 2020). A particularly important example are **indigenous data sovereignty rights**, see above 3.4 (GIDA 2018; Māori 2018; IWGIA 2020; USIDSN 2020).

### 4.3.4. Broader regimes of data access and access rights

Of late, and all the more with the mass roll-out of AI technologies, access to data beyond the data ownership debate has become a major policy issue. Access to data must not only be discussed with regard to individual actors, but also with a view to strong societies and economies, in particular data access by civil society (e.g., for accountability) and by academia (e.g., for research). The benefits of **open public sector data** are widely recognised (G8 2013; OECD 2018; OECD 2020). There is also increasingly a call for making this a two-way-road, obliging private players to share particular datasets with the public sector (**B2G data sharing**), such as to facilitate the development of smart cities, automated driving or traffic regulation (HLEG B2G 2020).

As to data sharing **between private parties**, there has been a general preference for incentivising **voluntary** data sharing, e.g. by laying down requirements for providers of data sharing services and entities collecting data for altruistic purposes to enhance public trust (EC 2020). **Mandatory** data sharing obligations have been introduced in specific sectors, and there may be more general obligations to share data in order to comply with the requirements of competition law/antitrust law. With only a few companies holding the bulk of some types of data available worldwide there have also been more far-reaching proposals of opening up privately held 'data silos', ranging from the introduction of new portability rights to the divestiture of mega companies in the data economy. As regards such access rights beyond co-generated data, the main criteria used from a policy-makers' perspective are **functionality**, namely to remedy a market failure, and **stakeholder interests** (Drexl 2017). In balancing these aspects, the principle of **proportionality** is being stressed, and more from a receiving party's perspective the further principles of reciprocity and avoidance of harm to the sharing party and others within that sharing party's sphere of interest (ALI & ELI 2020).

# 5. Roadmap for the Working Group

In the medium term, the GPAI Data Governance Working Group will deliver on three focal governance approaches: technical, legal, and organisational/institutional. The Working Group will, however, follow an integrated and holistic approach, i.e. not consider these three approaches as closed silos but rather cross-reference and link them as required by the relevant topic.

## 5.1. Technical approaches

There is a strong need for the **technical expertise** that goes into governance agreements, mechanisms, rules, and institutions to be identified separately from the usual private sector, civil-society and government components, even though – or all the more so given that – the technical subject-matter expertise may be found across all sectors. It very much defines the ways things can and cannot work and constitutes the 'physics', the 'plate tectonics' of these universes. Given the sheer complexity of managing data, the **use of technology** to enforce data governance requirements is essential. Technology can help govern data in several ways, including by helping create and maintain an understanding of the ownership, characteristics and flow of data within and across organisations; and by providing tools to meet data governance obligations across different stages of its lifecycle. Technology is required both to enhance and improve AI (e.g. bias detection software) and to create, in some cases, an AI-friendly technological environment (e.g. by ensuring machine-readability).

A review of the current state of technical approaches to data governance would include:

- machine- readability of data and metadata, including provenance data and dataset audit cards
- transparency and accountability enhancing technologies
- privacy enhancing technologies, including pseudonymisation and anonymisation techniques, federated machine learning, differential privacy, and the creation of synthetic data (including the schemes to produce them, such as video games)
- bias detection and correction techniques, including to support explainable AI
- technologies that support data access, controls and consent management (e.g individual data wallets), logging and auditing
- data interoperability, including standardisation of data formats and access and use of application programming interfaces (APIs)
- techniques to further implement digital sobriety and limit digital consumption
- Distributed Ledger Technologies (DLT)
- impact of emerging AI techniques (e.g. single shot and few shot learning, GANs, etc.)

## 5.2. Legal approaches

Data governance has to take many **different fields of the law** into account that need to be seen in context to achieve optimal results (e.g. data protection law, IP law, contract law, competition law). In this context, it is important to note that all these laws play a role, and maybe are in need of reform, to design data governance regimes that are fit for purpose. For instance, it is clear that, in particular, IP rights and rights such as the EU sui generis database right may have an adverse effect on data access, use and sharing. Any legal approach to data governance should rely both on statutory law and contracts, making use of a variety of **regulatory approaches**, including self-regulation and co-regulation. The legal dimension of data governance should also include the organisational/institutional aspects that are directly connected to legal frameworks and their implementation.

A review of the current state of legal approaches to data governance would include:

- intellectual intellectual property law as it applies to data, including collecting / generating / gathering data, deriving datasets, using and sharing data
- data protection law, in particular its application in the creation and use of AI
- human rights law and constitutional law
- legal recognition of data rights, notably in co-generated data
- data contract law and more broadly the law of data transactions, including third party effects of limitations on re-use
- legal and regulatory measures that enforce access to data and reuse of data, including freedom of information, reuse of public sector information, access by statistics agencies, city access to private data and data portability
- the use of voluntary mechanisms, certification, audit, codes of practice etc applied to data

## 5.3. Organisational/institutional approaches

Technical and legal approaches cannot unfold their potential without institutions and structures in place to implement them, including the appropriate operational schemes, and, where appropriate, economic aspects. These should provide frameworks that ensure optimal use of solutions and liberties, **empowering** individuals as well as communities and identifying the best articulations between the individual, local, regional, national, continental, and international levels. They should **facilitate** participation, **incentivise** desired behaviour, **ensure** sustainable development, and **yield** appropriate returns on investment as well as a fair share of everyone in the benefits of innovation and growth.

A review of the current state of organisational and institutional approaches to data governance would include approaches that focus on:

- individual data sovereignty and empowerment, such as personal data stores, representatives, trust schemes of different kinds, and cooperatives
- community data sovereignty and empowerment such as civic data trusts
- indigenous data sovereignty
- data access frameworks for research, innovation, and value creation, such as common data spaces
- smart cities, smart countries, collaborative maintenance of common assets
- corporate digital governance
- schemes for public and private enforcement of data rights and data law

# Annex: Data Governance Frameworks Worldwide

## United Nations

Draft for Consultation: Data Privacy Guidelines for the development and operation of Artificial Intelligence solutions (OHCHR 2020)
Roadmap for digital cooperation: implementation of the High-level panel on Digital cooperation (UN 2020)
Data Strategy of the Secretary-General for Action by Everyone, Everywhere (UN 2020)
Risks, Harms and Benefits Assessment Tool (UNGP 2020)
UN Global Pulse Annual Report 2019 (UNGP 2020)
OCHA Data Responsibility Guidelines (OCHA 2019)
Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda (UNDG 2017)
A Guide to Data Innovation for Development. From Idea to Proof-Of-Concept (UNGP 2016)
Integrating Big Data into the Monitoring and Evaluation of Development Programmes (UNGP 2016)

## OECD

Enhanced Access to Publicly Funded Data for Science, Technology and Innovation (OECD 2020)
Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies (OECD 2019)
OECD Council Recommendation on Artificial Intelligence (OECD 2019)
Open Government Data Report: Enhancing Policy Maturity for Sustainable Impact (OECD 2018)
Data-Driven Innovation: Big Data for Growth and Well-being (OECD 2015)

## Other International Frameworks

UNESCO, Access to Information: A new promise for sustainable development (UNESCO 2019)
G20 AI Principles (G20 2019)
UNESCO's Internet Universality Indicators: A Framework for Assessing Internet Development (UNESCO 2019)
International Open Data Charter (ODC 2015)

## Regional Frameworks

European Commission, Proposal for a Data Governance Act (EC 2020)
European Commission Communication, Building a European Health Union (EC 2020)
European Commission, Data Governance and Policies at the European Commission (EC 2020)
European Parliament, Draft Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (JURI 2020)
High-Level Expert Group on Business-to-Government data sharing, B2G Data Sharing Report (HLEG B2G 2020)
European Commission Communication, White Paper on Artificial Intelligence - A European approach to excellence and trust (EC 2020)
European Commission Communication, European Strategy for Data (EC 2020)
European Parliamentary Research Service, EU guidelines on ethics in artificial intelligence: Context and implementation (EPRS 2019)
European Union Agency for Fundamental Rights, Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights (FRA 2019)
High-Level Expert Group on AI, Policy and Investment Recommendations for Trustworthy AI (HLEG AI 2019)
High-Level Expert Group on AI, Ethics Guidelines for Trustworthy Artificial Intelligence (HLEG AI 2019)
Council of Europe, Addressing the impacts of Algorithms on Human Rights (CoE 2018)
ASEAN Telecommunications and Information Technology Ministers Meeting, Framework on Digital Data Governance (ASEAN 2018)
High-Level Expert Group on AI, Ethics Guidelines for Trustworthy Artificial Intelligence First Draft (HLEG AI 2018)
European Commission Communication, Towards a common European data space (EC 2018)
European Commission Staff Working Document, Guidance on Sharing Private Sector Data in the European Data Economy (EC 2018)
European Commission Communication, Building a European Data Economy (EC 2017)
European Commission Staff Working Document, Free Flow of Data and Emerging Issues of the European Data Economy (EC 2017)
Ibero-American Data Protection Network, Standards for Personal Data Protection for Ibero-American States (IADPN 2017)
European Commission Communication, Connectivity for a Competitive Digital Single Market - Towards a European Gigabit Society (EC 2016)
European Commission Staff Working Document, Accompanying the Communication on Connectivity for a Competitive Digital Single Market - Towards a European Gigabit Society (EC 2016)
European Commission Communication, Digitising European Industry – Reaping the full benefits of a Digital Single Market (EC 2016)
European Commission Staff Working Document, Advancing the Internet of Things in Europe Accompanying the document (EC 2016)
European Commission Communication, Towards a thriving data-driven economy (EC 2014)

## National Frameworks

*Australia:* Department of Industry, Science, Energy and Resources , AI Ethics Principles (Australia 2020)
*India:* Ministry of Electronics and Information Technology, Report by the Committee of Experts on Non-Personal Data Governance Framework (MEIT 2020)
*Japan:* Ministry of Economy, Trade and Industry, Governance Innovation: Redesigning Law and Architecture for Society 5.0 (METI 2020)
*Japan*: Ministry of Agriculture, Forestry and Fisheries Contract Guidelines on Utilization of AI and Data in Agriculture, Volumes 1: Know-how (MAFF 2020)

*Japan*: Ministry of Agriculture, Forestry and Fisheries Contract Guidelines on Utilization of AI and Data in Agriculture, Volume 2: Utilization of data (MAFF 2020)
*Japan*: Cabinet Office, Integrated Innovation Strategy 2020 (CO 2020)
*Japan*: Prime Minister's Office, Intellectual Property Promotion Plan 2020 (IPSA 2020)
*Japan:* Information Banking Certification for Application Guideline (ITF 2020)
*Singapore:* Info-communications Media Development Authority and
Personal Data Protection Commission, Model AI Governance Framework (PDPC 2020)
*UK:* Information Commissioner's Office, The principles to follow (ICO 2020)
*United Arab Emirates:* Smart Dubai, AI Ethics Principles and Guidelines (Dubai 2019)
*Germany:* Data Ethics Commission, Opinion of the Data Ethics Commission (DEK 2019)
*Japan*: Prime Minister's Office, AI Strategy 2019 (CO 2019)
*Japan:* Ministry of Agriculture, Forestry and Fisheries, Contract Guidelines on Utilization of Data in Industrial Safety Version 2 (METI 2019)
*Japan*: Ministry of Internal Affairs and Communications and Ministry of Agriculture, Forestry and Fisheries, Guidelines for Certification of Trust Function for Information Version 2.0 (MIAC & METI 2019)
*Japan*: Chief Information Officer, Guidelines for Online Identification in administrative procedure (CIO 2019)
*Japan*: Ministry of Agriculture, Forestry and Fisheries, Guidelines on "Shared Data with Limited Access" (METI 2019)
*Shanghai:* Municipal Commission of Economy and Informatization, Initiative for Artificial Intelligence Security Development (Shanghai 2019)
*U.S.A.:* Defense Innovation Board, AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense (DIB 2019)
*U.S.A.:* Executive Order on Maintaining American Leadership in Artificial Intelligence (White House 2019)
*Canada/France:* Joint Declaration on Artificial Intelligence (Canada & France 2018)
*Denmark:* Expert Group on Data Ethics, Data for the Benefit of the People: Recommendations from the Danish Expert Group on Data Ethics (EGDE 2018)
*Japan:* Ministry of Agriculture, Forestry and Fisheries, Contract Guidelines on Utilization of AI and Data Version 1.1 Formulated (METI 2018)
*Japan*: Ministry of Internal Affairs and Communications and Ministry of Agriculture, Forestry and Fisheries, Guidebook on Utilization of Camera Picture Data Version 2.0 (MIAC & METI 2018)
*Maori:* Māori Data Sovereignty Network, Principles of Māori Data Sovereignty (Māori 2018)
*U.K.:* Government Digital Service Data Ethics Framework (UKDS 2018)

## Academic, NGO and Private Sector Frameworks

ALI-ELI Principles for a Data Economy (ELI & ALI 2020)
Artificial Intelligence for Development in Africa (AI4D 2020)
Data's Ethical Charter for trustworthy development of the data economy (Occitanie 2020)
Essential requirements for establishing and operating data trusts: practical guidance co-developed by representatives from fifteen Canadian organizations and initiatives (IJPDS 2020)
Indigenous Data Governance Principles (USIDSN 2020)
Indigenous Data Sovereignty Initiative (IWGIA 2020)
Mind the Gap: The Final Report of the Equality Task Force (IFO 2020)
CARE Principles for Indigenous Data Governance (GIDA 2019)
Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems (IEEE 2019)
FAIR Guiding Principles for scientific data management and stewardship (GOFAIR 2019)
Beijing Academy AI Principles (BAAI 2019)
AI at Google: our principles (Google 2018)
Declaration on Ethics and Data Protection in Artificial Intelligence (ICDPPC 2018)
Guidelines for Artificial Intelligence (Deutsche Telekom 2018)
Accreditation criteria for data trading market operators (DTA Japan 2018)
IBM's Principles for Trust and Transparency (IBM 2018)
Montréal Declaration for a Responsible Development of Artificial Intelligence (Montréal 2018)
Responsible AI (Microsoft 2018)
The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems (Amnesty 2018)
Universal Guidelines for Artificial Intelligence (The Public Voice 2018)
Asilomar AI Principles (FLI 2017)
Statement on Algorithmic Transparency and Accountability (ACM 2017)
TOP 10 Principles for ethical artificial intelligence (UNI Global Union 2017)
Building Digital Trust: The role of data ethics in the digital age (Accenture 2016)
Principles for Accountable Algorithms and a Social Impact Statement for Algorithms (FATML 2016)
Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems (WEF 2014)

## Overview of Data Governance Frameworks in Literature

Jian C and Martin S, The Geopolitics of Data Governance: Data Governance Regimes (Oxford Insights 2020)
Rotenberg M, The AI Policy Sourcebook 2020 (Electronic Privacy Information Center 2020)
Manoj M, Big Data Governance Frameworks for 'Data Revolution for Sustainable Development' (Center for Internet & Society 2017)