Background Note

Overview of data principles

Version 3 — 5 August 2025

This document was prepared by the Secretariat at the request of the Working Group Chair to facilitate deliberations of the UN CSTD Working Group on Data Governance. The background note is a living document and will evolve based on feedback and inputs received from WG members and observers.

Contributions from Reyna Jenkyns, OECD, and UNHCR are gratefully acknowledged.

Contact: cstd-datagov@un.org

Introduction

Paragraph 48 of the Global Digital Compact identifies four areas where the Working Group may want to propose follow up recommendations. The first of these is 'fundamental principles of data governance at all levels as relevant for development'. To assist the WG membres in the discussion on this tòpic, this background note presents an initial list of **34 existing frameworks** on data governance principles. It focuses exclusively on principles relevant to international data governance arrangements applicable across various data types, sectors and thematic fields. These principles were developed by a diverse array of stakeholders, including bodies within the United Nations system, other intergovernmental and international organizations, academia, business and civil society.

Principles explicitly focused on internal organizational data governance practices detailing how individual entities collect, process, analyze, and store data for their internal operations were excluded. Nevertheless, internal principles for data governance may have broader implications. By establishing robust internal principles, organizations can lead by example, influencing the wider data governance landscape and potentially prompting data governance improvements beyond their immediate institutional environments. Despite acknowledging these valuable contributions, the Secretariat has chosen not to include such internal principles for data governance within the scope of this background note at this stage.

Similarly, national data governance principles were not included in this version of the background note.

Methodology

The Secretariat employed multiple analytical tools and targeted search strategies. Relevant data governance principles were systematically identified through search engines, policy document citations, academic literature, and submissions directly provided by intergovernmental and international organizations.

Recognizing that prominent data governance frameworks such as the FAIR and CARE principles originated within academic circles, the Secretariat extensively utilized scientific abstract and citation databases to expand the scope of the search. Specific combinations of key terms including "data," "data governance," "principle," "guideline," "recommendation," and "declaration" were applied across various bibliographic databases to achieve exhaustive coverage.

Furthermore, leveraging its professional expertise and networks, the Secretariat identified organizations likely to have publicly available data governance principles. Targeted searches were subsequently conducted on the websites of these entities.

This carefully curated selection aims to represent a diverse array of perspectives spanning different regions, sectors, and stakeholder groups, and may be added to during the Group's work in response to feedback from WG members.

List of data governance principles

1. UN CEB Data Principles
2. United Nations Fundamental Principles of Official Statistics
3. UNCTAD Data Principles for Development
4. UNICEF Responsible Data for Children (RD4C) Principles
5. UN Statistical Commission's Copenhagen Framework on Citizen Data
6. IASC Principles for Data Responsibility in Humanitarian Action
7. WHO Genomic Data Principles
8. African Union Data Policy Framework
9. APEC Data Principles
10. ASEAN Data Principles
11. ECOWAS Data Principles
12. Ibero-American Data Principles
13. ISO/IEC Data Principles
14. EU GDPR Data Principles
15. OAS Data Principles
16. OECD EASD principles
17. OECD Privacy Principles
18. OECD Good Practice Principles for Data Ethics in the Public Sector
19. Bitcom's Principles for the Data Governance Act
20. CARE Data Principles
21. Digital Development Principles
22. FAIR Data Principles
23. Feminist Data Principles
24. GEO Data Management Principles
25. Global Data Alliance's Cross-Border Data Policy Principles
26. Global Privacy Assembly (GPA) Principles
27. Lancet Commission Data Principles

28. Open Data Charter Principles
29. Open Government Data Principles
30. Ostrom’s principles
31. Santa Clara Principles
32. Transform Health Data Principles
33. TRUST Data Principles
34. WDS Data Sharing Principles

Matrix of data principles

This matrix provides a concise comparison of how the different frameworks emphasize specific data governance principles. Each framework reflects particular priorities related to its scope (e.g., health, human rights, privacy, indigenous sovereignty), but common themes like consent, transparency, accountability, and human rights frequently recur across frameworks.

Table 1. Commonalities and differences across selected data governance principles

Principles	UN CEB	UNFPOS	UNCTAD	UNICEF	UNStat	WHO	AUC	APEC	ASEAN	ECOWAS	IASC	Ibero-American
Human Rights	✓	Implicit	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Multi-stakeholder	Contextual	N/A	✓	✓	✓	✓	Contextual	Contextual	Contextual	Contextual	✓	Contextual
Context sensitivity	✓	✓	✓	✓	✓	✓	N/A	✓	✓	✓	✓	✓
Transparency	✓	✓	Implicit	Implicit	✓	✓	Implicit	✓	✓	✓	✓	✓
Accountability	✓	✓	Implicit	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data Security	✓	Implicit	Implicit	Implicit	✓	✓	✓	✓	✓	✓	✓	✓
Consent & User Control	Implicit	Implicit	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data Minimization & Proportionality	Contextual	Contextual	Implicit	✓	Contextual	Contextual	✓	✓	✓	✓	✓	✓
Equity & Non-Discrimination	✓	Implicit	✓	✓	✓	✓	✓	Contextual	Contextual	✓	✓	✓
Open Access & Data Sharing	✓	✓	Implicit	Implicit	✓	✓	✓	Implicit	Implicit	Implicit	Implicit	Implicit
Data Quality & Interoperability	✓	✓	Contextual	Contextual	✓	✓	✓	✓	✓	✓	✓	✓
Innovation	Contextual	N/A	✓	N/A	Contextual	Contextual	Contextual	Contextual	Contextual	Contextual	N/A	Contextual

Legend:

✓ Explicitly stated as a core principle.

Implicit Implied or indirectly supported.

Contextual Addressed in specific contexts or dependent on interpretation.

N/A Not applicable.

Table 1. Commonalities and differences across selected data governance principles (continued)

Principle	ISO/IEC	GDPR	OAS	OECD EASD	OECD Privacy	OECD Public Sector	Bitcom	CARE	Digital Dev.	FAIR	Feminist
Human Rights	Implicit	✓	Implicit	✓	Implicit	Implicit	N/A	✓	✓	N/A	✓
Multi-stakeholder	Contextual	N/A	N/A	N/A	N/A	N/A	✓	Implicit	✓	N/A	✓
Context sensitivity	N/A	N/A	Contextual	✓	Implicit	Implicit	Implicit	✓	✓	N/A	✓
Transparency	✓	Implicit	✓	✓	Implicit	N/A	✓	✓	✓	Contextual	✓
Accountability	✓	✓	✓	✓	✓	Implicit	✓	✓	✓	Contextual	✓
Data Security	✓	✓	✓	✓	✓	N/A	✓	Contextual	Contextual	N/A	Contextual
Consent & User Control	N/A	✓	✓	✓	✓	✓	N/A	✓	✓	N/A	✓
Data Minimization & Proportionality	✓	✓	Implicit	✓	✓	✓	✓	Implicit	✓	N/A	Contextual
Equity & Non-Discrimination	Contextual	✓	Contextual	✓	Contextual	Contextual	N/A	✓	✓	Contextual	✓
Open Access & Data Sharing	Contextual	Implicit	Implicit	✓	Contextual	✓	✓	Contextual	✓	✓	Contextual
Data Quality & Interoperability	✓	Implicit	✓	✓	✓	✓	✓	Contextual	Contextual	✓	Contextual
Innovation	Contextual	Contextual	Contextual	✓	Contextual	N/A	✓	Contextual	Contextual	N/A	Contextual

Table 1. Commonalities and differences across selected data governance principles (continued)

Principle	GEO	Global Data Alliance	GPA	Lancet	Open Data Charter	OGD	Ostrom	Santa Clara	Transform Health	TRUST	WDS
Human Rights	N/A	N/A	✓	✓	Contextual	Contextual	Implicit	✓	✓	Implicit	Implicit
Multi-stakeholder	N/A	Contextual	Contextual	Contextual	✓	✓	✓	✓	✓	✓	N/A
Context sensitivity	N/A	N/A	✓	✓	Contextual	Contextual	N/A	✓	✓	✓	✓
Transparency	✓	Implicit	✓	✓	✓	✓	✓	✓	✓	✓	✓
Accountability	✓	✓	✓	✓	Contextual	Contextual	✓	✓	✓	✓	✓
Data Security	N/A	Implicit	✓	Contextual	Contextual	Contextual	N/A	Contextual	✓	✓	✓
Consent & User Control	N/A	Implicit	✓	✓	Contextual	Contextual	✓	✓	✓	Implicit	Implicit
Data Minimization & Proportionality	N/A	N/A	✓	Contextual	Contextual	Contextual	Contextual	Contextual	✓	Implicit	Implicit
Equity & Non-Discrimination	N/A	✓	✓	✓	✓	Contextual	Contextual	✓	✓	Implicit	Implicit
Open Access & Data Sharing	✓	Implicit	Implicit	✓	✓	✓	Contextual	Contextual	✓	✓	✓
Data Quality & Interoperability	✓	✓	✓	✓	✓	✓	Contextual	Contextual	Contextual	✓	✓
Innovation	N/A	Implicit	Contextual	✓	Contextual	Contextual	Contextual	Contextual	✓	Contextual	N/A

ANNEX. Compendium of data governance principles

UN CEB Data Principles

The UN Chief Executives Board elucidate data principles to achieve three overarching goals: value, trust and equity. To maximise value, the principles urge governments, businesses and civil society to create enabling environments in which data are accessible, interoperable and reusable across borders, while cultivating a culture of "mutuality and solidarity" so the benefits of data flow to all communities.

According to UN CEB, the goals and principles should:

- Be forward-thinking and adaptable, while fostering consistency in data governance across international actors and countries;

- Be appropriate to the context: in terms of the data type and its use, and ensuring its relevance and effectiveness in diverse settings;

- Promote equitable access to data for sustainable development and ensure that data benefit all;

- Support, promote and be aligned with globally recognized frameworks and objectives, such as international human rights and the Sustainable Development Goals;

- Be aligned with and support shared goals, such as value, trust and equity;

- Support the adoption of a multi-stakeholder approach that brings together diverse stakeholders and mobilizes support for complex policy reforms and interventions.

These principles provide practical and ethical guidelines and serve as guidance for the design and development of future global data governance, and for evaluating its effectiveness.

Value: Maximizing the value of data requires:

- An enabling environment for data use and reuse. Foster a culture and systems (i.e. processes, methods and tools) that value and promote appropriate access and responsible use and reuse of data (e.g. with the adoption of responsible open data standards). This principle includes providing equal access to the benefits of data and the related technologies, devices and tools. This principle also envisages educating and empowering individuals, communities and organizations to produce or co-create, work with, inform decisions with, derive benefits from and understand data effectively;

- Interoperability. Promote data interoperability and portability by adopting standardized and open formats, common metadata elements that enable data transfer and reuse, protocols, taxonomies and interfaces. This principle can contribute to improved consistency and integration across different systems, both to enable effective data collaboration and sharing and to simplify the extraction and compilation of data from multiple sources;

- Mutuality and solidarity. Encourage data governance approaches that prioritize mutual benefit and solidarity for people across geography and generations so that data can be

used for the greater good of society, considering both individual and collective needs, interests and responsibilities.

Trust: Enabling trust requires:

- A human rights-based approach to data. Respect, protect and promote human rights and fundamental freedoms, as defined in international human rights law. This should apply across all elements of data governance, including data protection and privacy, in particular for children or other vulnerable groups who may not be in a position to make determinations for themselves and must rely on others to act in their best interests. This principle emphasizes the need for a fair and legitimate approach to processing, purpose specification, proportionality and necessity, retention, accuracy, confidentiality, security, transparency, transfers and accountability;

- Accountability. Articulate clear accountabilities, roles and responsibilities over data assets and processes, including assigning responsibility to explain outcomes and to ensure that individuals can access and control their data. Appropriate oversight, impact assessment, audit and due diligence mechanisms should be put in place to ensure accountability. In addition, data subjects must have clear rights of redress to ensure accountability. Governance structures should enhance ethical and legal responsibility and accountability at every stage of the data life cycle;

- Data quality. Take the measures necessary to ensure data quality throughout the data life cycle. This involves treating data in context (i.e. using them with an understanding of the context and conditions in which they were produced), ensuring that accurate, reliable, timely data and metadata are available, and promoting

- Data security and infrastructure protection. Safeguard the infrastructure and systems for data over the entire life cycle, from design and collection to use, transfer and sharing, dissemination, and archiving and destruction to ensure the security and integrity of data and data flows. This principle involves implementing appropriate organizational and technical safeguards, procedures and systems to prevent, mitigate, report and respond to security breaches or misuse of data (including unauthorized or inappropriate internal access or manipulation, accidental disclosure, damage, alteration, loss and other security risks related to data management).

Equity: Promoting equity in data governance requires:

- Digital self-determination. Recognize the principle of digital selfdetermination, empowering individuals and communities to have control over their personal data and its uses. This principle involves enabling individuals to make informed decisions about their data and to exercise their right to access, correct, delete and agree to the purposes of data processing and use;

- Fairness and non-discrimination. Reduce data poverty and correct for bias and discrimination throughout the data life cycle, and take measures to promote the fair distribution of data benefits and avoid the unfair distribution of data risks. This principle includes responsible open and equal access to data, as well as improved disaggregation, where relevant, to describe and understand specific characteristics, leaving no one behind;

- People-centred. Ensure that people are at the centre of data governance decision-making. Empower people to access, analyse and use data through inclusive and participatory decision-making and better assess the risks and implications of data issues. Consultation should be meaningful, identifying and testing underlying assumptions, determining benefits, capacities, risks, harms and adverse impacts, and adopting prevention and mitigation measures;

- Data stewardship. Establish and resource responsible data stewardship frameworks (with appropriately skilled capacities) to properly manage, curate and protect data and to maximize data use and reuse for the public good.

UN Fundamental Principles of Official Statistics (UNFPOS)

The Fundamental Principles of Official Statistics, endorsed by the United Nations, provide an essential framework for producing and disseminating reliable, high-quality statistics.

Principle 1: Relevance, Impartiality, and Equal Access: Official statistics provide an indispensable element in the information system of a democratic society, serving the Government, the economy and the public with data about the economic, demographic, social and environmental situation. To this end, official statistics that meet the test of practical utility are to be compiled and made available on an impartial basis by official statistical agencies to honour citizens' entitlement to public information.

Principle 2: Professional Standards, Scientific Principles, and Professional Ethics: To retain trust in official statistics, the statistical agencies need to decide according to strictly professional considerations, including scientific principles and professional ethics, on the methods and procedures for the collection, processing, storage and presentation of statistical data.

Principle 3: Accountability and Transparency: To facilitate a correct interpretation of the data, the statistical agencies are to present information according to scientific standards on the sources, methods and procedures of the statistics.

Principle 4: Prevention of Misuse: The statistical agencies are entitled to comment on erroneous interpretation and misuse of statistics.

Principle 5: Sources of Official Statistics: Data for statistical purposes may be drawn from all types of sources, be they statistical surveys or administrative records. Statistical agencies are to choose the source with regard to quality, timeliness, costs and the burden on respondents.

Principle 6: Confidentiality: Individual data collected by statistical agencies for statistical compilation, whether they refer to natural or legal persons, are to be strictly confidential and used exclusively for statistical purposes.

Principle 7: Legislation: The laws, regulations and measures under which the statistical systems operate are to be made public.

Principle 8: National Coordination: Coordination among statistical agencies within countries is essential to achieve consistency and efficiency in the statistical system.

Principle 9: Use of International Standards: The use by statistical agencies in each country of international concepts, classifications and methods promotes the consistency and efficiency of statistical systems at all official levels.

Principle 10: International Cooperation: Bilateral and multilateral cooperation in statistics contributes to the improvement of systems of official statistics in all countries.

UNCTAD Data Principles for Development

In February 2024, UN Trade and Development (UNCTAD) published seven principles of data governance for development, consistent with the imperatives of multilateralism, multi-stakeholder approach and multidisciplinary consideration of data:

1. *Foundation in human rights.* Data governance should be consistent with the Universal Declaration of Human Rights, upholding human rights in all aspects of data management and use.

2. *Treating data in context.* As products of socio-technological systems, data are neither objective nor neutral. They reflect pre-existing social relations and technological limitations, making this context essential for ensuring the ethical design of data-based decisions.

3. *Balancing risks and innovation*. It is crucial for data governance to balance risk aversion with innovation promotion. This involves recognizing and addressing risks inherent in data management, while simultaneously supporting and not unduly hindering data-driven innovations.

4. *Empowering people.* To empower individuals, it is essential to enhance data skills and capabilities and provide access to data infrastructures and effective tools for data management, while protecting indigenous knowledge. These efforts should enable people to make informed decisions about their data and fully benefit from technological progress.

5. *Multilayered approach in data governance.* Data governance should strike a balance between hard (legally binding) and soft law (guidelines and practices) mechanisms. This multilayered approach leverages the strengths of each, providing a robust yet flexible framework that can adapt to the evolving data landscape.

6. *Multi-stakeholder inclusivity.* Effective data governance requires a multi-stakeholder approach. This includes engaging policymakers, businesses, academia, nongovernmental organizations, technical communities, civil society and other relevant groups. Excluding any stakeholder group can compromise the effectiveness and fairness of data governance.

7. *Inclusion of youth for future orientation.* Finally, data governance should proactively incorporate youth perspectives. This helps in designing forward-looking, people-centred, inclusive and development-oriented information society. Inclusion of youth ensures that data governance is aligned with the aspirations and needs of future generations.

UNICEF Responsible Data for Children (RD4C) Principles

UNICEF established a set of principles designed to guide how data concerning children are collected, shared, and used. The principles aim to ensure that data work for and not against children's well-being, rights, and agency. Recognizing that children are uniquely vulnerable and often underrepresented in decision-making about data, the principles promote a rights-based, context-sensitive, and participatory approach to data governance in child-focused work:

1. **Purpose-Driven:** A responsible data practice starts by being purpose-driven. When seeking to handle data actors should identify and specify why the data is needed and how the intended or potential benefits relate to improving children's lives. If there is no clearly articulated benefit for children, actors should not collect data, store, share or analyze it.

2. **People-Centric:** Much of the data used for drawing insights to improve children's lives involves or is generated by people. The insights from it have the potential to impact the lives of children in many ways, both positive and negative. Actors must thus ensure the needs, interests and expectations of people, including children and their caregivers in particular, are prioritized by those handling data about them. Actors should take a people-centric approach to the consideration of opportunities and risks of data initiatives, prioritizing the consideration of data practices' effects on people over potential efficiency gains or other process-oriented objectives. This entails some combination of the following criteria: children and/or their caregivers have consented to the data use, children and/or their caregivers have a clear understanding of how this work will be conducted, the work is demonstrably serving children's interests, and/or the work is required by law or institutional mandate. In addition, actors need to be context sensitive, paying attention to and acting according to the legal, cultural and community contexts in which any given project exists.

3. **Participatory**: Responsible data is participatory. It seeks and builds with inputs from those who use and are affected by data, namely children, their caregivers, and the communities in which they live. Accordingly, actors should inform and engage with individuals and groups. In seeking input, actors should pay attention to marginalized and vulnerable population segments as well as to the inputs of partners, donors and other key stakeholders.

4. **Protective of Children's Rights:** When it comes to children, responsible data practices begin by recognizing their distinct needs and requirements. Children's rights must be realized in order for them to develop to their full potential. Realizing these rights can be complex given children's inherent vulnerabilities, the likelihood that others are making impactful decisions on their behalf, and the future prospects they can achieve if supported effectively by those working in their interest.

5. **Proportional:** In the data space, less can sometimes be more. When developing and implementing data initiatives, actors should always consider necessity and whether there is proportionality in the breadth of data collection and duration of data retention in order to achieve the intended purpose. The collection and retention of data should be relevant, limited and adequate to what is necessary for achieving intended purposes. The importance of targeting and minimizing collection is true of all data, but especially true of data related to children, given potential and actual vulnerabilities.

6. **Professionally Accountable:** Data responsibility rests upon broader foundations of professional accountability. To ensure that the practices and principles described above are

put in action, and the unique considerations of responsible data for children are operationalized within institutional processes, organizations and partners should collect, process, and use data within a more general culture of data responsibility. Such a culture has many elements, but one of the most important is to establish and clearly define the role of organization-wide data stewards. Data stewards are an emerging role; they are individuals or groups whose duties cut across departments and functions, and whose broad remit is to oversee responsibility and accountability in the way data is handled.

7. **Prevention of Harms across the Data Life Cycle:** Data is not static but exists on a cycle. As part of a commitment to data responsibility, actors should assess and seek to prevent risks across the full data life cycle, including the collecting, storing and preparing, sharing, analyzing and using stages. This concept is called end-to-end data responsibility. It is essential for preventing harm to children and ensuring trust.

UN Statistical Commission's Copenhagen Framework on Citizen Data

The UN Statistical Commission's Copenhagen Framework on Citizen Data outlines ten core principles to guide the responsible, ethical, and rights-based production and use of citizen data. These principles aim to safeguard individuals and communities, particularly in contexts where non-state actors or civil society organizations engage in data collection:

1. **Independence**: Data collection must be free from political interference to ensure objectivity and integrity.

2. **Relevance**: Data should directly address issues that matter to citizens and the communities or civil society organizations that represent them.

3. **Participation and Informed Consent**: All relevant groups, including marginalized and vulnerable populations, must be meaningfully involved, with individuals giving informed, voluntary consent and retaining control over their data.

4. **Professional Standards**: Data must be collected, processed, and disseminated according to professional and scientific standards to ensure quality, usability, and societal value.

5. **Data Security**: Protections must be in place to safeguard data, including clear rules on copyright, intellectual property, and data sharing.

6. **Self-Definition and Self-Identification**: Populations of interest must define themselves, and personal attributes should be self-identified by individuals, respecting personal autonomy.

7. **Transparency**: Metadata and paradata (e.g., methods, collection design) should be openly available to enable understanding and scrutiny of how data are collected and used.

8. **Ethical and Safe Production and Use**: Data activities must prioritize human rights, dignity, and the principle of "do no harm," avoiding discrimination or stigmatization.

9. **Confidentiality, Privacy, and Data Attribution**: Personal data must remain confidential, used strictly for statistical purposes, and never disclosed in ways that could identify individuals.

10. **Openness and Accessibility**: Data should be made publicly available in open formats and accessible to all, including persons with disabilities and those with limited access to technology.

WHO Genomic Data Principles

The World Health Organization (WHO) has established a set of principles to guide the ethical collection, access, use, and sharing of human genomic data to uphold human rights, promote social justice, and ensure equitable and responsible use of genomic information across contexts and communities:

1. **Affirming and Valuing Rights:** Individuals with decision-making capacity must have the right to make informed choices about their genomic data throughout the data lifecycle. For those without such capacity, their best interests must be protected, and community and family views must be respected.

2. **Social Justice:** Genomic data practices should promote health and well-being, reduce inequalities, address the needs of underserved populations, and prevent discrimination and stigmatization. Capacity-building and equitable resource distribution are essential.

3. **Solidarity:** Emphasizes standing together in ensuring fair access to genomic data and equitable sharing of its benefits and burdens, addressing global and local disparities in data-related capacities.

4. **Equitable Access and Benefit-Sharing:** Commitment to ensuring all individuals and communities can benefit fairly from genomic data, with intentional efforts to correct imbalances in representation, power, and participation in governance and datasets.

5. **Collaboration, Cooperation, and Partnership:** Promotes inclusive and mutually beneficial collaboration across local, national, and international levels, including public–private partnerships, with efforts to rebalance power among stakeholders.

6. **Stewardship of Human Genome Data:** Calls for the responsible management of genomic data through ethical, legal, culturally appropriate processes that reduce risks, follow best practices, and respect privacy laws and norms.

7. **Transparency:** Requires clear, accessible information on how genomic data are collected, used, and protected, along with a commitment to sharing research findings with those who contributed data.

8. **Accountability:** Demands mechanisms to ensure responsible data practices, including consequences for misuse and failure to comply with established ethical standards.

African Union Data Policy Framework

The African Union Commission's Data Policy Framework outlines a set of data governance principles designed to foster a unified, equitable, and secure African digital ecosystem. A key operational sub-principle of the AUC Data Policy Framework is data minimisation, which aims to limit the collection of personal data to what is strictly necessary, thereby reducing risks to individuals. Additionally, AUC advocates for alignment of data processing frameworks with established data protection norms, including consent and legitimacy, purpose limitation, data quality, security safeguards, openness (including incident reporting), accountability, and data specificity.

1. **Cooperation:** African Union Member States shall cooperate in exchanging data, acknowledging data as a central input of the global economy and the importance of the interoperability of data systems to a flourishing African digital single market.

2. **Integration:** The Framework shall promote intra-Africa data flows, remove legal barriers to data flow, subject only to necessary security, human rights and data protection.

3. **Fairness and inclusiveness:** In the implementation of the Framework, Member States shall ensure it is inclusive and equitable, offering opportunities and benefits to all Africans, and in so doing, seek to redress national and global inequalities by being responsive to the voices of those marginalised by technological developments.

4. **Trust, safety and accountability:** Member States shall promote trustworthy data environments that are safe and secure, accountable to data subjects, and ethical and secure by design.

5. **Sovereignty:** Member States, AUC, Regional Economic Communities, African Institutions and International Organisations shall cooperate to create capacity to enable African countries to self-manage their data, take advantage of data flows and govern data appropriately.

6. **Comprehensive and forward-looking:** the Framework shall enable the creation of an environment that encourages investment and innovation through the development of infrastructure, human capacity and the harmonisation of regulations and legislation.

7. **Integrity and justice:** Member States shall ensure data collection, processing and usage are just and lawful, and data should not be used to discriminate unfairly or infringe peoples' rights.

APEC Data Principles

The APEC Privacy Framework and its accompanying Data Governance Principles guide data governance and privacy practices across the Asia-Pacific region, emphasizing trust, cross-border cooperation, innovation, and individual rights. Developed by the Asia-Pacific Economic Cooperation (APEC) forum, these principles support economic integration while promoting responsible and accountable data handling among APEC member economies.

While there is no single “APEC Data Governance Principles” document separate from its privacy frameworks, the key principles can be understood from the APEC Privacy Framework (updated in 2015) and its supporting instruments like the Cross-Border Privacy Rules (CBPR) System. The principles below reflect the core data governance approach promoted by APEC:

1. **Preventing Harm:** Organizations should prevent misuse of personal information that could lead to harm to individuals, including reputational, financial, or discriminatory harm.

2. **Notice:** Individuals should be informed about data collection practices, including what is collected, why, and how it will be used or disclosed.

3. **Collection Limitation:** Data should be collected only as necessary and by lawful and fair means.

4. **Use of Personal Information:** Personal data should be used only for the purposes specified at the time of collection or for compatible purposes with user consent.

5. **Choice:** Individuals should have meaningful choices regarding the collection, use, and disclosure of their personal information.

6. **Integrity of Personal Information:** Organizations should ensure that personal information is accurate, complete, and kept up to date.

7. **Security Safeguards:** Reasonable security measures should protect personal information against unauthorized access, destruction, or loss.

8. **Access and Correction:** Individuals should be able to access their personal data and request corrections where necessary.

9. **Accountability:** Organizations that collect and control personal information are accountable for complying with these principles, including through internal procedures and oversight.

ASEAN Data Principles

The ASEAN Framework on Personal Data Protection (ASEAN PDP Framework) establishes a regional baseline for protecting individuals' personal data, recognizing the importance of preventing its misuse and fostering trust in the digital economy. It outlines key principles that ASEAN Member States are encouraged to incorporate into their domestic laws and regulations:

1. **Consent, Notification, and Purpose:** Personal data should only be collected, used, or disclosed with the individual's consent after being informed of the purpose, unless otherwise authorized or required by law. The purpose must be appropriate and reasonable under the circumstances.

2. **Accuracy of Personal Data:** Personal data must be accurate and complete to the extent necessary for the purposes for which it is collected, used, or disclosed.

3. **Security Safeguards:** Personal data must be protected against risks such as loss, and unauthorized access, use, disclosure, modification, or destruction.

4. **Access and Correction:** Individuals should be able to request access to their personal data and have errors or omissions corrected, unless legal exceptions apply.

5. **Transfers to Another Country or Territory:** Before transferring data internationally, organizations must either obtain the individual's consent or ensure the recipient offers comparable levels of data protection.

6. **Retention:** Organizations should cease to retain personal data, or anonymize it, when it is no longer necessary for legal or business purposes.

7. **Accountability:** Organizations must be responsible for complying with the principles and must provide accessible information about their data protection policies and contact points.

ECOWAS Data Principles

The ECOWAS Act on Personal Data Protection sets out a structured and rights-based approach to personal data governance, articulating a series of principles that guide lawful and ethical data processing within the ECOWAS region:

- **Consent and Legitimacy**: Data processing is legitimate when the data subject gives informed consent. However, consent is not required in cases of legal obligation, public interest, contract performance, or protection of vital interests.

- **Legality and Fairness**: All processing activities must be conducted lawfully, fairly, and without deception or fraud.

- **Purpose, Relevance, and Preservation**: Data must be collected for specified, explicit, and lawful purposes, and not processed in ways incompatible with those purposes. It must be relevant to the purpose and not retained longer than necessary, except for legitimate historical, statistical, or research uses under legal conditions.

- **Accuracy**: Personal data must be accurate and kept up to date. Reasonable efforts must be made to correct or erase data that is inaccurate or incomplete.

- **Transparency**: Data subjects must be informed about how their personal data are being processed, reinforcing openness and accountability.

- **Confidentiality and Security**: Data must be processed securely and kept confidential, especially during transmission over networks, to protect against unauthorized access or breaches.

- **Choice of Data Processor**: When data controllers delegate processing, they must choose processors that provide sufficient guarantees for data protection. Both parties are jointly responsible for ensuring compliance with security obligations.

- **Specific Principles (Sensitive Data)**: The processing of sensitive categories of data (such as those revealing racial or ethnic origin, political opinions, religious beliefs, health status, or sexual life) is strictly prohibited within the ECOWAS region.

IASC Principles for Data Responsibility in Humanitarian Action

IASC Principles for Data Responsibility in Humanitarian Action were developed by the Data Responsibility Working Group (DRWG), a global coordination body working to advance data responsibility across the humanitarian system. DRWG brings together a diverse group of stakeholders including United Nations entities, other International Organizations, Non-Governmental Organizations (NGOs), and other stakeholders engaged in the coordination and implementation of humanitarian action and/or operational data management. The DRWG began as an Inter-Agency Standing Committee (IASC) Sub-Group in 2020 and transitioned into a system-wide working group in early 2021. The primary aim of the DRWG is to advance data responsibility as the approach to operational data management at all levels of the humanitarian system, primarily through the lens of the IASC Operational Guidance on Data Responsibility in Humanitarian Action (first released in February 2021 and revised in April 2023).

1. **Accountability** In accordance with relevant applicable rules, humanitarian organizations have an obligation to accept responsibility and be accountable for their data management activities. Humanitarian organizations are accountable to affected populations, to internal governance structures, and to national, regional and international actors and authorities, as applicable. Humanitarian organizations should put in place all measures required to achieve their accountability commitments in line with these Principles. Such measures include establishing adequate policies, guidance, and processes, and ensuring that sufficient and appropriate competencies and capacities are available, including but not limited to financial, human and technological resources. Establishing competencies and capacities should include offering training and learning opportunities to ensure that staff have the expertise, skills, knowledge and attitudes needed to manage data responsibly

2. **Confidentiality**: Humanitarian organizations should implement appropriate organizational safeguards and procedures to keep sensitive data confidential at all times, including through clear and consistent access restrictions. Measures should be in line with applicable organizational policies and legal requirements, while taking into account the relevant data and information sensitivity classification system(s) in the response context.

3. **Coordination and Collaboration:** Coordinated and collaborative data management entails the meaningful inclusion of humanitarian partners, national and local authorities, people affected by crisis, and other stakeholders in data management activities, where appropriate and without compromising the humanitarian principles or this Operational Guidance. Humanitarian organizations should coordinate and collaborate to ensure that appropriate connections are established between humanitarian operational data management activities and longer-term development-oriented data processes and data investments. Local and national capacity should be strengthened wherever possible, and not be undermined.

4. **Data Security:** Humanitarian organizations should implement appropriate organizational and technical safeguards, procedures and systems to prevent, mitigate, report and respond to security breaches of both digital and non-digital data. These measures should be designed to protect against material external breaches as well as unauthorized or inappropriate internal access or manipulation, accidental disclosure, damage, alteration, loss, and other security risks related to data management. Measures should be based

on the sensitivity of the data and updated as data security standards and best practice evolve.

5. **Defined Purpose, Necessity and Proportionality:** Humanitarian data management and its related activities should have a clearly defined purpose. The design of processes and systems for data management should contribute to improved humanitarian outcomes, be consistent with relevant mandates, respect and promote rights and freedoms, and carefully balance those where needed. In line with the concept of data minimization, the management of data in humanitarian response should be relevant, limited and proportionate to the specified purpose(s).

6. **Fairness and Legitimacy:** Humanitarian organizations should manage data in a fair and legitimate manner. Fair data management enables the delivery of humanitarian action in a neutral and impartial manner. Legitimate grounds for data management include, for example: the best and/or vital interests of communities and individuals affected by crisis, consistent with the organization's mandate; public interest in furtherance of the organization's mandate; and any other legitimate ground specifically identified by an organization's regulatory framework and/or applicable laws.

7. **Human Rights-Based Approach:** Data management should be designed and implemented in ways that respect, protect and promote the fulfillment of human rights, including fundamental freedoms and the principles of equality and non-discrimination as defined in human rights frameworks, as well as data-specific rights promulgated in applicable legislation.

8. **People-Centered and Inclusive:** Affected populations should be afforded an opportunity to participate and be included, represented, and empowered to exercise agency in all steps of data management for a given activity, whenever the operational context permits. The human autonomy of people affected by crisis should guide humanitarian data management. Special efforts should be made to support the participation and engagement of people who are not well represented or may be marginalized in a given data management activity (e.g., due to age, gender and other diversity characteristics such as disability, ethnicity, religion or sexual orientation), or are otherwise 'invisible', consistent with commitments to leave no one behind. These should include fostering data literacy across and within communities.

9. **Personal Data Protection:** When managing personal data, humanitarian organizations have an obligation to adhere to (i) applicable national and regional data protection laws, or (ii) if they enjoy privileges and immunities such that national and regional laws do not apply to them, to their own data protection policies.These laws and policies contain the principles for personal data protection, such as a list of equally valid legal bases for the processing of personal data, including but not limited to consent. Humanitarian organizations subject to national or regional legislation should also take into account the guidelines and advisories issued by relevant data protection authorities within their applicable jurisdiction. When designing data management systems, humanitarian organizations should meet the standards of privacy and data protection by design and by default. Humanitarian organizations should take personal data protection into consideration when developing open data frameworks. In line with their commitment to ensure accountability to affected people, inclusivity and respect for human rights, humanitarian organizations should uphold data subjects' rights to be informed, in an

easily accessible and appropriate manner, about the processing of their personal data, to be able to request to access, correct, delete, object to or request information about the processing of their personal data, and to not be subject to automated decision-making except under the specific conditions set out in the legal frameworks applicable to an organization.

10. **Quality:** Data quality should be maintained such that the owners, users and other key stakeholders are able to trust data management activities and their resulting products. Data quality entails that data is relevant, accurate, timely, complete, standardized, interoperable, well-documented, up-to-date and interpretable, in line with the intended use and bearing in mind the given operational context. Where feasible and appropriate, and without compromising these Principles, organizations should strive to collect and analyze data by age, sex and disability disaggregation, as well as by other diversity characteristics as relevant to the defined purpose(s) of an activity.

11. **Retention and Destruction:** Organizations should establish a data retention and destruction schedule that indicates how long data will be retained and when data should be destroyed, as well as how to do so in a way that renders data retrieval impossible. Sensitive data should only be retained for as long as it is necessary to the specified purpose(s) for which it is managed or as required by applicable laws or audit regulations. When retaining sensitive data, organizations should specify and ensure its safe and secure storage to prevent misuse or exposure. Non-sensitive data may be retained indefinitely, in line with applicable laws, regulations and policies, and provided that access rights are established and the sensitivity of the data is reassessed on a regular basis.

12. **Transparency:** Organizations should manage data in ways that offer meaningful transparency toward humanitarian actors and stakeholders, particularly affected populations. This should include the provision of timely and accurate information about the data management activity such as its purpose(s), the intended use(s) of and approaches to sharing the data, as well as any associated limitations and risks.

Ibero-American Data Principles

The Ibero-American Standards for the Protection of Personal Data establish a rights-based framework for personal data governance across Ibero-American states, grounded in a set of comprehensive principles. These include:

- **Legitimation**: Data may be processed only under specific lawful bases, such as consent, legal obligation, vital interests, public interest, or legitimate interest that does not override the data subject's fundamental rights.

- **Lawfulness**: Processing must fully comply with domestic and international legal standards and safeguard individuals' rights and freedoms.

- **Loyalty**: Processing must prioritize the data subject's best interests and avoid deception or discriminatory outcomes.

- **Transparency**: Data subjects must be clearly and accessibly informed about data processing practices, including the controller's identity, processing purposes, rights mechanisms, and potential recipients.

- **Purpose**: Data must be collected for specific, legitimate, and explicit purposes and not repurposed in ways incompatible with the original intent.

- **Proportionality**: Only the minimum data necessary for the intended purpose should be processed.

- **Quality**: Data must be accurate, up to date, and kept only for as long as necessary. It must be safely deleted or anonymized when no longer required.

- **Responsibility**: Controllers must demonstrate accountability and compliance through internal policies, audits, training, and mechanisms to respond to rights requests and complaints.

- **Safety**: Adequate administrative, technical, and physical safeguards must be implemented to ensure data confidentiality, integrity, and availability, proportionate to risks and the nature of the data.

- **Confidentiality**: All persons involved in data processing must uphold confidentiality, even after the end of their relationship with the controller.

ISO/IEC Data Principles

The ISO/IEC 38505-1:2017 standard, developed by the International Organization for Standardization and the International Electrotechnical Commission, provides guiding principles for members of governing bodies on the effective, efficient, and acceptable use of data within their organizations. It addresses the governance of both current and future use of data that are created, collected, stored, or controlled by IT systems, and informs management processes and decision-making related to data. A revised version of this standard, ISO/IEC CD 38505-1, is currently under development and will eventually replace the 2017 edition.

The ISO/IEC 38505-1:2017 standard defines data governance as a domain within IT governance, which in turn is a subset of broader organizational governance. ISO/IEC 38505-1:2017 builds upon the governance principles set out in ISO/IEC 38500, the foundational international standard for IT governance, adapting and applying them specifically to the context of data. The standard offers both public and private sector organizations essential criteria to evaluate decisions related to the collection, storage, sharing, and use of data:

1. **Responsibility:** Every data-related activity must have a clearly designated owner accountable for ensuring ethical, lawful, and efficient execution. Governing bodies must delegate authority consistent with defined responsibilities and enforce clear escalation procedures for handling exceptions.

2. **Strategy:** Organisations should have a documented data strategy that aligns current and future data activities with their overarching goals, delivering measurable value. Boards should assess whether proposed data initiatives (such as analytics, artificial intelligence, or data sharing) are consistent with strategic objectives and transparently address trade-offs between value creation and associated risks.

3. **Acquisition:** Decisions to acquire data must be grounded in a clear business case and should thoroughly evaluate cost-benefit analyses, data provenance, quality, and rights of use. Governing bodies must ensure management applies rigorous due diligence concerning consent, intellectual property rights, jurisdictional limitations, and vendor dependencies.

4. **Performance:** Data must consistently meet quality standards: accuracy, timeliness, accessibility, security, and interoperability. Boards should establish key performance indicators (KPIs), such as data-quality metrics, speed of insight delivery, and adherence to service levels, and require regular reporting to verify compliance.

5. **Conformance:** Governance practices must ensure adherence to external regulations (e.g., laws, sector-specific requirements, contractual obligations) and internal policies on information security, privacy, and data retention. Independent audits, internal control evaluations, and tracking of corrective actions are essential governance mechanisms.

6. **Human Behaviour:** Effective data governance should actively consider human factors such as skills development, incentives, ethical standards, change management, and communication. Governing bodies must ensure supportive practices, including training programs, awareness initiatives, and behavioural controls, to foster responsible and trustworthy data handling.

EU GDPR Data Principles

The General Data Protection Regulation (GDPR) outlines seven fundamental principles that organizations must follow when processing personal data. These principles ensure data protection practices are ethical, transparent, and accountable. Specifically, the GDPR mandates:

1. **Lawfulness, Fairness, and Transparency:** Data processing must have a valid legal basis, respect the rights of data subjects, and clearly communicate how data is used.

2. **Purpose Limitation:** Personal data should only be collected and processed for explicitly stated and legitimate purposes, without unauthorized reuse.

3. **Data Minimisation:** Organizations must only gather and process data that is strictly necessary for the intended purpose.

4. **Accuracy:** Personal data must be accurate and kept up to date, with processes in place for timely correction or deletion of incorrect information.

5. **Storage Limitation:** Data should not be stored longer than necessary, and mechanisms must exist to securely delete data when it is no longer needed.

6. **Integrity and Confidentiality:** Adequate security measures must protect personal data against unauthorized access, alteration, or disclosure, maintaining data integrity and confidentiality.

7. **Accountability:** Organizations must be able to demonstrate compliance with these principles through proper documentation, training, and accountability mechanisms.

OAS Data Principles

The Organization of American States (OAS) has developed a set of principles on privacy and personal data protection. These principles aim to protect individual privacy while facilitating legitimate data processing within the region.

1. **Lawful Purposes and Loyalty:** Data processing must be lawful and based on a legitimate purpose.

2. **Transparency and Consent:** Individuals should be informed about data collection and processing, and their consent should be obtained where necessary.

3. **Relevance and Necessity:** Data should be relevant to the intended purpose and collected only to the extent necessary.

4. **Limited Processing and Retention:** Processing should be limited to the specific purpose and retained only for as long as necessary.

5. **Confidentiality:** Data should be kept confidential and protected from unauthorized access.

6. **Security of Data:** Appropriate security measures should be in place to protect data from unauthorized access and loss.

7. **Accuracy of Data:** Data should be accurate and kept up-to-date.

8. **Access, Rectification, Erasure, Objection, and Portability:** Individuals should have rights to access, rectify, erase, object to, and port their data.

9. **Sensitive Personal Data:** Special protection is needed for sensitive personal data, such as religious, political, or biometric data.

10. **Accountability:** Data controllers should be accountable for their actions and must implement measures to comply with these principles.

11. **Trans-Border Flow of Data and Accountability:** Safeguards are needed to ensure the safe and secure transfer of data across borders.

12. **Data Protection Authorities:** There should be designated authorities to oversee and enforce these principles.

13. **Exceptions:** There may be exceptions to these principles in specific circumstances, such as national security or law enforcement.

OECD EASD Principles

The OECD Recommendation on Enhancing Access to and Sharing of Data (EASD) sets out "*general principles and policy guidance on how governments can maximise the benefits of enhancing data access and sharing arrangements while protecting individuals' and organisations' rights and taking into account other legitimate interests and objectives.*" It is structured along **three overarching objectives** (Sections 1-3), encompassing **seven general principles,** each accompanied with actionable policy recommendations for their implementation and complemented by a set of key definitions. The principles include:

Section 1 - "Reinforcing Trust across the Data Ecosystem"

1. **Empowerment and pro-active engagement**

- Inclusive participation of all relevant actors, including vulnerable or marginalised groups;
- Competition-neutral data-sharing partnerships, including Public-Private Partnerships;
- Transparency and responsible data practices throughout the data value cycle;
- Empowerment of individuals, social groups, and organisations through enhanced agency and control;

2. **Whole-of-government approach and leadership**

- Prioritisation of data access and sharing initiatives aligned with public interest objectives;
- Coherence, flexibility and scalability of policy frameworks, including national data strategies, and their regular reviews;
- Effective policy coordination and implementation across government with multi-stakeholder participation;
- Technology-neutrality and agility of legal and regulatory environments with the necessary legal certainty and protection;

3. **Maximising the benefits of data, while protecting rights and other legitimate interests**

- Making data as open as possible and as closed as necessary;
- Necessity and proportionality of measures to protect legitimate public and private interests;
- Clear accountability of stakeholders according to their roles, including for data security and quality;
- Conditioned data access and sharing via effective technological and organisational means;

Section 2 - "Stimulating Investment in Data and Incentivising Data Access and Sharing"

1. **Incentives and sustainable investment**

- Effective competition in data markets;
- Self- or co-regulation mechanisms, where appropriate;
- Long-term investments to ensure sustainability of data arrangements;
- Fair distribution of benefits through appropriate incentive mechanisms;
- Development and upscaling of new business models and application areas;

Section 3 - "Fostering Effective and Responsible Data Access, Sharing, and Use Across Society"

1. Cross-border data access and sharing with trust

- Minimisation of restrictions to cross-border data access and sharing, especially for purposes of global public interest;
- Non-discriminatory, transparent, necessary, and proportionate measures for conditioning cross-border data access and sharing;
- Continued international co-operation and dialogue across jurisdictions;

2. Findability, accessibility, interoperability and reusability (FAIR) of data across organisations

- Transparent and timely provision of data together with required meta-data, documentation, models, and algorithms, supported by appropriate access control mechanisms;
- Interoperable and open specifications including common standards, for data formats and models;

3. Capacity building for effectively using data responsibly along the data value cycle

- Awareness about the benefits and risks to encourage responsible data governance;
- Data-related skills and competencies including citizen's data literacy and capacity to understand data governance issues and exert their rights;
- Access to, and adoption of, sustainable, open, scalable, safe, and secure foundational infrastructures needed along the data value cycle.

OECD Privacy Principles

The OECD Privacy Principles are captured by the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, first issued in 1980 and updated in 2013.

- **Collection Limitation Principle:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

- **Data Quality Principle:** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

- **Purpose Specification Principle:** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

- **Limitation Principle:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law.

- **Security Safeguards Principle:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

- **Openness Principle:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

- **Individual Participation Principle:** Individuals should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; b) to have communicated to them, data relating to them i. within a reasonable time; ii. at a charge, if any, that is not excessive; iii. in a reasonable manner; and iv. in a form that is readily intelligible to them; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

- **Accountability Principle:** A data controller should be accountable for complying with measures which give effect to the principles stated above.

OECD Good Practice Principles for Data Ethics in the Public Sector

At the heart of the OECD Good Practice Principles for Data Ethics in the Public Sector lies a dedication to fostering the ethical use of data within the public sector. The aim is to ensure that digital government initiatives, projects, products, and services are not only effective but also worthy of the trust citizens place in their governments. These principles provide a framework to guide public officials, organizations, and decision-makers in embedding data ethics into every facet of their operations:

1. Manage data with integrity;

2. Be aware of and observe relevant government-wide arrangements for trustworthy data access, sharing and use;

3. Incorporate data ethical considerations into governmental, organisational and public sector decision-making processes;

4. Monitor and retain control over data inputs, in particular those used to inform the development and training of AI systems, and adopt a risk-based approach to the automation of decisions;

5. Be specific about the purpose of data use, especially in the case of personal data;

6. Define boundaries for data collection, access, sharing and use;

7. Be clear, inclusive and open;

8. Publish open data and source code;

9. Be accountable and proactive in managing risks

Bitkom's Principles for the Data Governance Act

The Bitkom framework (Germany's digital association) provides guidance for shaping a robust and innovation-friendly data governance environment, particularly through its detailed response to the European Commission's Data Governance Act (DGA). Bitkom emphasizes the need for clear, harmonized frameworks that encourage innovation while ensuring data protection and security. It calls for balanced regulations that promote fair competition, voluntary data sharing, and interoperability across sectors.

Bitkom's key principles for data governance include:

1. **Regulatory Framework: Enable innovation-friendly data economy:** Establish innovation-friendly regulations that complement strong data protection by encouraging self-determined, and contract-based data handling to promote free and fair competition between all market players.

2. **Data spaces: Taking different setups and structures into account:** Create diverse data governance structures tailored to specific sectoral needs while ensuring interoperability among these spaces without overly restrictive regulations and limiting other possible setups of data spaces.

3. **Specify definition and scope: Be aware of sector specificities:** Clearly define data transmission types and scopes, respecting sector-specific practices and ensuring regulations complement existing functional models.

4. **Access to public data: Building a comprehensive, coherent and systematic framework:** Build a comprehensive, coherent system for open government data sharing, standardizing metadata and formats to avoid fragmentation and ensure broad accessibility.

5. **Interoperability and data transfer: Balance Standardization and Agility:** Balance standardization with innovation, applying standards selectively to mature technologies and fostering experimental flexibility for emerging data handling methods.

6. **Framework for data intermediaries: Focus on what is actually needed in the market:** Develop a regulatory framework that incentivizes trust and neutrality for intermediaries without imposing excessive regulatory burdens, enabling additional value-added services.

7. **Framework for Data Altruism: Make it work by providing legal basis:** Create clear legal foundations for data altruism, facilitating voluntary data sharing for public good and addressing regulatory complexities.

8. **Allow for free flow of data: Improve legal certainty:** Ensure legal certainty for cross-border data flows, minimizing restrictions and clearly defining exceptions, particularly concerning mixed and non-personal datasets.

9. **IP: Shielding provisions and their implementation require legal clarity:** Provide clarity regarding IP provisions, ensuring alignment with international agreements (e.g., the Berne Convention, the TRIPs agreement) and transparent adequacy decisions for data transfers.

10. **A streamlined enforcement structure: Avoid bureaucratic overload:** Implement efficient, agile oversight structures to avoid bureaucratic bottlenecks, promoting swift decision-making and harmonized enforcement.

11. **Connect with existing rules and initiatives: Building a coherent framework:** Integrate and align data governance frameworks, fostering coherence and maximizing interoperability among data governance projects.

12. **Ensure strategic foresight: Take future developments into account:** Anticipate future technological developments, designing agile, transparent, and secure frameworks that promote innovation and openness in emerging data-based technologies.

CARE Data Principles

The CARE Principles for Indigenous Data Governance provide a framework to ensure that the rights, interests, and values of Indigenous Peoples are respected in the collection, use, and reuse of data related to them, their communities, lands, and knowledge systems.

C – Collective Benefit

Data use should result in tangible, inclusive benefits for Indigenous communities. This includes advancing self-determined development, enhancing governance, and achieving equitable outcomes. Data ecosystems must be designed to support Indigenous-led innovation and uphold community-defined values.

A – Authority to Control

Indigenous Peoples have the inherent right to govern the collection, access, use, and sharing of data about their peoples, cultures, lands, and resources. This right is grounded in Indigenous Data Sovereignty and reaffirmed by instruments like the UN Declaration on the Rights of Indigenous Peoples (UNDRIP). Indigenous nations must be recognized as data rights-holders, not merely stakeholders.

R – Responsibility

Non-Indigenous data holders have a duty to engage respectfully and collaboratively with Indigenous communities, ensuring that data practices strengthen capacity, uphold cultural heritage, and support language revitalization. Responsibility also means acknowledging and addressing historical injustices and promoting equitable data partnerships.

E – Ethics

The use of Indigenous data must be guided by Indigenous ethical frameworks, which prioritize justice, harm reduction, benefit maximization, and sustainability. Ethical stewardship requires that data use aligns with community values over time, ensuring accountability and adaptability to future generations.

The CARE Principles are designed to be complementary to the FAIR Principles, Findable, Accessible, Interoperable, Reusable, and other mainstream data frameworks, and promote equitable participation and outcomes from data access, use, reuse, and attribution in contemporary data landscapes (Carroll et al., 2021).

Principles for Digital Development

The Principles for Digital Development are a set of nine community-driven guidelines that support inclusive, sustainable, and ethical digital development. Originally launched in 2014 and refreshed in 2024, the principles serve as a compass for policymakers, technologists, and practitioners working across diverse sectors and geographies to design, implement, and govern digital systems that maximize positive outcomes while minimizing harm. These principles recognize that digital systems shape societies and emphasize the importance of radical inclusion, local ownership, ethical data use, and open innovation:

1. **Understand the existing ecosystem:** Ground digital work in the realities of existing technological, social, political, and cultural contexts.

2. **Share, reuse, and improve**: Promote collaboration and open innovation by building on existing tools, approaches, and resources.

3. **Design with people**: Engage users and stakeholders meaningfully throughout the design and implementation process.

4. **Design for inclusion**: Ensure that digital tools and systems are accessible and equitable for all, particularly marginalized communities.

5. **Build for sustainability**: Develop solutions that can endure over time in terms of resourcing, maintenance, and adaptability.

6. **Establish people-first data practices**: Collect, manage, and use data ethically, prioritizing the rights, privacy, and agency of individuals and communities.

7. **Create open and transparent practices**: Foster trust and accountability through openness in design, governance, and communication.

8. **Anticipate and mitigate harms**: Identify and address potential risks or unintended consequences before they materialize.

9. **Use evidence to improve outcomes**: Ground decisions in data, learning, and research to continuously refine and strengthen impact.

FAIR Data Principles

The FAIR Data Principles provide a widely adopted framework for improving the management, stewardship, and reuse of research data. First published in 2016 by a group of data experts (Wilkinson et al., 2016) and endorsed by international organizations, the principles aim to **to** improve discovery, access, integration and usability of data, both by machines and by human beings.

F – Findable

Data should be easy to locate by both humans and machines. This requires the assignment of globally unique and persistent identifiers (such as DOIs), and the inclusion of rich metadata that clearly describe the data and are indexed in searchable repositories or registries.

A – Accessible

Once found, data should be retrievable using standardized communication protocols (e.g., HTTP or FTP), which are open, free, and universally implementable. Access should be clearly defined—whether data are open or restricted—and metadata should remain accessible even if the data are no longer available.

I – Interoperable

Data should be structured using standard formats, vocabularies, and ontologies so they can be combined with other datasets and work across different systems. Metadata should use common languages and standards to enable seamless integration into various applications, platforms, and disciplines.

R – Reusable

To ensure that data can be reused in the future, it should be described in a way that includes clear licensing, provenance, and contextual information. This supports proper attribution and enables data to be used across different research questions and settings.

Feminist Data Principles

Feminist data principles, also known as the principles of data feminism, are a framework for analyzing and challenging power dynamics in data collection, analysis, and interpretation (D'Ignazio & Klein, 2023). They aim to make data practices more equitable and inclusive, particularly for marginalized groups:

1. **Examine Power:** This principle focuses on identifying and understanding how power operates in data systems, including how it shapes data collection, analysis, and interpretation. It involves recognizing biases and inequalities embedded in data and algorithms.

2. **Challenge Power:** This principle calls for actively challenging power structures and inequalities in data practices. It encourages pushing back against systems that perpetuate oppression and working towards more just and equitable outcomes.

3. **Elevate Emotion and Embodiment:** This principle emphasizes the importance of incorporating emotions and lived experiences into data analysis. It recognizes that data is not solely objective and that feelings, embodied knowledge, and personal experiences are valuable sources of information.

4. **Rethink Binaries and Hierarchies:** This principle encourages challenging binary thinking (e.g., gender binary) and hierarchical structures that can perpetuate discrimination. It promotes the inclusion of diverse perspectives and experiences in data analysis.

5. **Embrace Pluralism:** This principle advocates for valuing multiple perspectives and voices in data analysis. It encourages diversity of thought and knowledge in the data science process.

6. **Consider Context:** This principle emphasizes the importance of understanding the social, historical, and political context in which data is collected and analyzed. It recognizes that data is not neutral and that it is shaped by power dynamics.

7. **Make Labor Visible:** This principle highlights the invisible labor involved in data collection, analysis, and interpretation. It acknowledges the work that goes into creating data and the importance of giving credit and recognition to all those involved in the process.

GEO Data Management Principles

The Group on Earth Observations (GEO) Data Management Principles establish a comprehensive framework to ensure that Earth Observation data are discoverable, accessible, usable, preserved, and curated in alignment with international best practices. First developed in 2015 and revised in 2024, these principles support the effective implementation of the GEO Data Sharing Principles and complement widely adopted frameworks such as the FAIR, TRUST, and CARE Principles. The GEO Data Management Principles (DMPs) are intended to guide all stakeholders (especially data providers) in managing data throughout their lifecycle to promote interoperability, transparency, and long-term stewardship. They apply to all types of Earth Observation data and services, including raw data, Analysis Ready Data, and on-demand data products, with guidance provided for implementation, evaluation, and self-assessment:

1. **Metadata for Discovery**: Data and metadata will be discoverable through catalogues and search engines, with clear information on access conditions, including licenses.

2. **Online Access:** Data will be accessible via online services, at minimum through direct download, and preferably via customizable services for visualization and analysis.

3. **Data Encoding**: Data will be structured using widely accepted, preferably non-proprietary, standards aligned with user community needs and observing methods.

4. **Data Documentation**: Data will be comprehensively documented through structured metadata, based on international or community standards, and supplemented by peer-reviewed publications where possible.

5. **Data Traceability**: Data will include provenance metadata indicating origin and processing history to ensure traceability and reproducibility.

6. **Data Quality Control**: Data will undergo quality control, with results recorded in metadata; unchecked data will be flagged accordingly.

7. **Data Preservation**: Data will be preserved for long-term use, with protection from loss, including planning for retention, disposal, and disaster recovery.

8. **Data and Metadata Verification**: Data and metadata will be periodically verified for integrity, authenticity, and readability.

9. **Data Review and Reprocessing**: Data will be curated through correction, updating, and reprocessing as appropriate, following agreed procedures.

10. **Persistent and Resolvable Identifiers**: Data will be assigned persistent, unique, and resolvable identifiers to support citation, credit, and data traceability.

Global Data Alliance's Cross-Border Data Policy Principles

The Global Data Alliance's Cross-Border Data Policy Principles emphasize the importance of seamless, secure, and responsible data flows to foster innovation, economic growth, and employment. Recognizing the detrimental effects of data protectionism, the Alliance advocates for transparent, accountable, and interoperable policies to strengthen international consensus and digital trust.

Global Data Alliance's key principles for cross-border data transfers include:

1. **Countries should maintain the longstanding presumption favoring the seamless and responsible movement of data across borders:** This presumption reflects the reality of international economic relations today: Data moves seamlessly and securely across globally or regionally distributed cloud-based digital networks that do not match up neatly with national boundaries.

2. **Any rules impacting cross-border data transfers should be developed and maintained in accordance with good regulatory practices:** The second pillar of an international policy consensus on data transfers involves transparent, accountable, and evidence-driven regulatory practices. Adhering to these practices helps ensure that any rules impacting cross-border data are well justified, enjoy the support and trust of the public, and do not unintentionally harm international commerce and innovation. In the design, development, issuance, implementation, and review of measures that may impact cross-border data transfers, governments should: Be transparent; Draw from the best reasonably available evidence relevant to the proposed cross-border data policy; Analyze that evidence according to sound, objective, and verifiable methods; Provide opportunity for input from the public, experts, and interested stakeholders; and Include other procedural safeguards and due process.

3. **Any rules impacting cross-border data transfers should be non-discriminatory:** The third pillar supporting an international policy consensus on data transfers requires a commitment to principles of nondiscrimination and national treatment in terms of the nationality of persons, products, services, or technologies. Subject to legitimate public policy limitations, a rule impacting cross-border data transfers would raise concerns if it distorted the market or altered conditions of competition based on the national origin of the persons, the products or services, or the technologies involved. In some cases, concerns may also arise if data transfer rules are designed to provide economic advantages to transfers within a country's borders, and to domestic persons, their products or services, or their technologies, than are afforded to cross-border transfers and non-national persons, products, services, or technologies. Likewise, countries should refrain from discriminatory treatment among sectors, for example by blocking or impeding data transfers in particular sectors.

4. **Any rules impacting cross-border data transfers should be necessary to achieve a legitimate objective and not impose greater restrictions than necessary:** This standard is reflected in many RTAs negotiated to date and in the administrative and regulatory processes adopted by many governments. As part of their administrative and regulatory practice, governments typically evaluate costs, benefits, and reasonably available alternatives as part of their assessment of whether proposed rules are necessary to achieve a specific public policy objective. Often referred to as regulatory impact assessments, these regulatory evaluations are particularly salient to data transfer restrictions, which can result in excessive economic costs and impacts. Such assessments should evaluate from a cross-border policy perspective: The particular public policy outcome that the proposed measure is intended to achieve; Whether the cross-border data restrictive features of the proposed measure are needed to achieve that outcome; Whether other regulatory or non-regulatory alternatives could feasibly address that need or achieve that outcome with fewer data transfer restrictions; The potential impacts of various

alternatives over time (e.g., economic, social, environmental, public health, and safety effects) on the government, enterprises, and other persons who depend upon the ability to access technologies and transfer data across borders; The grounds for concluding that a particular policy alternative is preferable to others.

5. **Countries should support the use of accountability models aligned with international best practices to foster responsible data transfer practices:** The fifth pillar incorporates the accountability model, first established by the Organisation for Economic Co-operation and Development (OECD) and subsequently endorsed and integrated into other legal systems and privacy principles. This model provides an approach to cross-border data governance that effectively protects the individual and fosters streamlined, robust data transfers. Under legal frameworks that adopt the accountability model, organizations are required to implement procedures to ensure that data they transfer outside of the country continues to be protected, regardless of where it is stored.

6. **Countries should work together to create compatible trust-based frameworks support the seamless and responsible movement of information across borders:** Continuing to enjoy the transformative benefits enabled by the seamless and responsible movement of data requires a commitment to digital trust. Building digital trust requires both domestic and international action. That means domestic and international legal frameworks help economies realize the benefits of cross-border data transfers and cloud-based technology without sacrificing expectations of privacy, security, and safety.

Global Privacy Assembly (GPA) Principles

The Global Privacy Assembly (GPA) principles on data protection and privacy articulate a comprehensive framework for safeguarding personal data in an increasingly complex digital environment:

1. Lawfulness and Fairness: Processing must comply with national laws and international agreements. It must also be fair, avoiding deceitful or fraudulent collection and ensuring no discriminatory or biased outcomes.

2. Purpose Specification: Personal data should be collected and used only for specific, explicit, and legitimate purposes and not repurposed in ways incompatible with those purposes.

3. Necessity and Proportionality: Data processing must be limited to what is necessary and proportionate to achieve its objectives, especially when involving sensitive data or emerging technologies.

4. Data Quality: All reasonable steps must be taken to ensure that personal data is accurate and up to date, especially when it informs automated or algorithmic decisions.

5. Retention/Storage Limitation: Personal data should only be retained as long as necessary for the stated purposes and should be deleted or anonymised when no longer needed.

6. Transparency: Individuals must be clearly and accessibly informed about how their data is processed, by whom, and for what purposes, with mechanisms tailored to different contexts.

7. Accountability: Data controllers must take proactive measures to ensure and demonstrate compliance with data protection obligations, embedding accountability into operations.

8. Security: Controllers and processors must implement appropriate safeguards to ensure the confidentiality, integrity, and availability of data, addressing increasing cybersecurity threats.

9. Legitimacy and Bases for Processing: Processing must have a lawful basis (e.g., consent, contract, public interest), and where consent is used, it must be freely given, specific, informed, and unambiguous.

10. Sensitive Data: Enhanced protections are required for sensitive personal data (e.g., health, biometric, political opinions), including consideration of how non-sensitive data might become sensitive when combined.

11. Protection for Children and Vulnerable People: Special safeguards are necessary for individuals less able to understand or exercise their data rights, such as children and vulnerable populations.

12. Controllers and Processors: Clear arrangements must be in place between controllers and processors, including roles, responsibilities, and contractual processing terms.

13. International Transfers of Personal Data: Cross-border data transfers must be safeguarded using tools like adequacy decisions, standard clauses, and certifications to ensure protection follows the data.

14. Right to Information: Individuals have the right to be informed about what data is collected, how it is used, by whom, and what rights they have, especially in complex

automated systems.

15. Rights of Access, Rectification, Deletion, and Objection: Individuals must be able to access their data, correct inaccuracies, request deletion, and object to processing when appropriate.

16. Restriction: Individuals must have the right to restrict processing, particularly when data is inaccurate, contested, or processed unlawfully.

17. Data Portability: People should be able to obtain their personal data in a commonly used electronic format and transfer it to another provider or service.

18. Rights Relating to Profiling and Automated Decisions: Individuals affected by automated decisions must be informed, allowed to seek human review, and be able to challenge such decisions.

19. Ability to Exercise Rights: Simple and efficient mechanisms must be in place to allow individuals to exercise their rights. Any restrictions must be lawful and proportionate.

20. Proactive Measures: Organizations must implement privacy by design and by default, conduct impact assessments, provide training, and adopt internal policies and breach response protocols.

21. Supervisory Authority: An independent, well-resourced, and technically competent authority must oversee and enforce data protection laws and promote awareness.

22. Cooperation: Data protection authorities should collaborate with each other and with other regulators (e.g., competition, cybersecurity) to ensure consistent and effective regulation.

23. Liability and Redress: Legal frameworks should provide for accountability and allow individuals to enforce their rights and seek remedies through the courts.

Lancet Commission Data Principles

The Lancet and Financial Times Commission on Governing Health Futures 2030 outlines a set of data principles that frame the ethical and equitable governance of health data in an increasingly digital world:

1. **Data Solidarity:** This approach emphasizes building a culture of data justice and equity, where the value of data is used for the public good while respecting individual rights.

2. **Equitable Access and Use:** The commission advocates for equitable opportunities for accessing and using health data, while simultaneously respecting individual privacy.

3. **Data Governance and Transparency:** The commission calls for the establishment of data institutions to govern the exchange and storage of health data, as well as transparency in how data sharing and use will improve public and individual health.

4. **Data Integration:** The principles encourage the generation of data that can be integrated into patient records and national monitoring indicators.

5. **Standards-Based Approach:** The commission promotes a standards-based approach to increase system interoperability and reduce potential conflicts and confusion.

6. **Patient-Centred Care:** Recognizing the importance of patient preferences, needs, and values in all clinical decisions.

Open Data Charter Principles

The Open Data Charter outlines six core principles designed to guide governments and organizations in making data open, accessible, and reusable to drive innovation, transparency, and inclusive development. Launched in 2015 and adopted by governments, and organizations worldwide, the Open Data Charter's principles reflect a commitment to data openness as a means to achieve broader public policy goals:

1. **Open By Default:** This represents a real shift in how government operates and how it interacts with citizens. At the moment, we often have to ask officials for the specific information we want. Open by default turns this on its head and says that there should be a presumption of publication for all.

2. **Timely and Comprehensive:** Open data is only valuable if it is still relevant. Getting information published quickly and in a comprehensive way is central to its potential for success. As much as possible governments should provide data in its original, unmodified form.

3. **Accessible and Usable:** Ensuring that data is machine readable and easy to find will make data go further. Portals are one way of achieving this. But it's also important to think about the user experience of those accessing data, including the file formats that information is provided.

4. **Comparable and Interoperable:** Data has a multiplier effect. The more quality datasets you have access to, and the easier it is for them to talk to each other, the more potential value you can get from them. Commonly agreed data standards play a crucial role in making this happen.

5. **For Improved Governance & Citizen Engagement:** Open data has the capacity to let citizens (and others in government) have a better idea of what officials and politicians are doing. This transparency can improve public services and help hold governments to account.

6. **For Inclusive Development and Innovation:** Finally, open data can help spur inclusive economic development. For example, greater access to data can make farming more efficient, or it can be used to tackle climate change.

Open Government Data Principles

The Open Government Data (OGD) Principles establish a foundational framework for determining whether government data can be considered truly open. These principles are rooted in ensuring data produced or held by governments is accessible, usable, and reusable by all.

1. **Complete**: All public data should be made available, with the only limitations being those necessary to protect privacy, security, or legally privileged information. This ensures that openness is the default, not the exception.

2. **Primary**: Data should be provided in its original, raw form as collected at the source, maintaining the highest possible level of detail. This enables more accurate analysis and reuse for diverse purposes, avoiding the bias or loss of detail that can occur in pre-processed datasets.

3. **Timely**: Data must be released as quickly as needed to retain its relevance and value. Timely access is especially crucial for data with implications for public decision-making, emergency response, or service delivery.

4. **Accessible**: Data should be made available in ways that are usable by the broadest possible audience, without unnecessary technical or financial barriers. This includes ensuring usability across different platforms and demographics.

5. **Machine Processable**: To facilitate automated analysis, data must be structured in a format that computers can efficiently read and process, supporting innovation in services, applications, and policy evaluation.

6. **Non-discriminatory**: Data access should be open to all, without requiring registration, membership, or credentials. This ensures fairness and maximizes the potential for civic and commercial use.

7. **Non-proprietary**: Data should be published in formats that are free from control by any private entity, supporting interoperability and ensuring that no one has exclusive rights to access or manipulate the data.

8. **License-free**: Data should not be subject to intellectual property restrictions. It must be free to use, reuse, and redistribute, subject only to limitations needed for privacy, security, or confidentiality.

Ostrom's principles

Elinor Ostrom's framework for the management of shared resources (Ostrom, 1990) offers valuable insights for the regulation and governance of data (Coyle et al., 2020). Ostrom's work addresses situations where collective agreement is necessary to manage access to and the use of shared resources, particularly when individual interests must be balanced against broader societal benefits. This framework is especially relevant for data governance. Ostrom's design principles and their data economy parallels help illuminate the challenges presented by asymmetries in information and incomplete regulatory agreements common in the data economy. They offer practical guidelines for defining access rights, establishing accountability mechanisms, and promoting socially beneficial uses of data:

1. **There are clear boundaries and rules about who is entitled to what:** Individuals with rights to access and manage data must be explicitly identified, and the scope and limits of data resources clearly defined, guided by shared purposes and values. Rules governing data access, use, and contribution should be tailored to specific conditions, ensuring fairness and proportional benefits for contributors while minimizing potential harm.

2. **Monitoring actions is feasible:** Transparency and auditability of how data is being collected, used and shared. Data governance must involve continuous monitoring by stakeholders or accountable parties, ensuring compliance with established governance frameworks and mechanisms.

3. **There are mechanisms for resolving conflicts:** Effective and accessible mechanisms for resolving disputes related to data governance should be available, clearly outlining internal resolutions and conditions requiring external mediation or legal intervention.

4. **Individual responsibilities and benefits broadly balance:** Transparency and better understanding of both rights and how value from data returns to people and organisations

5. **Users themselves are responsible for monitoring and enforcement:** Decision-making processes regarding data governance should include participation from those affected, fostering collective agreement and legitimacy in rule formation.

6. **Sanctions for abuse are possible and graduated, getting progressively tougher:** A structured system of graduated sanctions should be implemented to enforce data governance rules, accounting for factors like intent and the degree of harm resulting from violations.

7. **Decisions are legitimated by the participation of users:** For individuals, consent and opt outs need to be informed and viable (which requires competitive alternative services).

8. **Decisions are also legitimated by government recognition:** A comprehensive data strategy and regulatory framework are essential. Individuals and communities governing data resources must have their autonomy recognized and supported by external authorities, aligning internal governance practices with broader regulatory frameworks like data protection laws.

Santa Clara Principles

The Santa Clara Principles on Transparency and Accountability in Content Moderation are a globally recognized framework developed to guide tech companies and governments in making digital content moderation more transparent, rights-respecting, and accountable. They originated in 2018 and were significantly expanded in 2022 following global consultations with civil society, affected communities, and experts.

The principles are organized into **three core categories**:

1. Foundational Principles

These principles embed a rights-based framework into content moderation systems:

- **Human Rights and Due Process:** Companies must integrate human rights (especially freedom of expression and non-discrimination) and due process at all stages of content moderation, ensuring fair enforcement and meaningful recourse for users. Use of automation should be limited to high-confidence, human rights-considerate contexts.

- **Understandable Rules and Policies:** Rules must be clearly written, publicly accessible, and understandable, with detailed guidance and examples of permitted and prohibited content and enforcement mechanisms (e.g., takedowns, downranking).

- **Cultural Competence:** Content moderation decisions should reflect awareness of language, culture, and local context. Users must be able to interact with policies and appeals in their own language and trust that moderation reflects their sociocultural realities.

- **State Involvement in Content Moderation:** Companies must be transparent about any role state actors play in flagging, influencing, or requiring enforcement actions, especially where censorship or abuse of power may be at play.

- **Integrity and Explainability:** Content moderation systems (especially automated ones) must be reliable, explainable, regularly audited, and open to independent scrutiny. Users should understand how algorithmic systems affect them and be able to request human review.

2. Operational Principles

These principles outline practical standards for how companies should implement transparent moderation processes:

- **Numbers:** Detailed transparency reporting must be standard. This includes total content actions, appeals, outcomes, and disaggregated data by country, language, type of violation, source of flagging (e.g. users, bots, governments), and use of automation. Reports should be machine-readable and regularly updated.

- **Notice:** Users whose content is acted upon should receive timely and clear notices, including the reason for the decision, how it was flagged, and whether a government

was involved. Notices should include a path for appeal, be persistent (accessible even if accounts are suspended), and available in the user's language.

- **Appeal:** Users must have a meaningful opportunity to challenge content or account actions. This includes:

    a) Clear, accessible appeals processes

    b) Timely human review by someone not involved in the original decision

    c) Consideration of language and context

    d) Notifications of outcomes and rationales

Expedited appeals should be possible in high-impact cases (e.g., elections or targeted harassment).

3. Principles for Governments and State Actors

- **Removing Barriers to Company Transparency:** States should not block companies from disclosing data on government takedown requests. Any such limitations must be legally justified and narrowly tailored.

- **Promoting Government Transparency:** Governments should themselves be transparent about content moderation demands, including:

    a) Frequency and legal basis of takedown requests

    b) Publicly reporting involvement by courts, law enforcement, or regulators

    c) Encouraging company transparency through supportive regulation

Transform Health Data Principles

The Health Data Governance Principles, stewarded by Transform Health and developed with broad civil society engagement, are structured around three overarching objectives: **Protect People**, **Promote Health Value**, and **Prioritize Equity**. They are not prioritized hierarchically but are mutually reinforcing and accompanied by practical core tenets.

1. Protect People: Health data governance must safeguard individuals and communities from harm throughout the data lifecycle, especially considering the sensitivity of health data.

- **Protect individuals and communities** through purpose-driven data collection, limited collection of sensitive data, secure storage and sharing, and mitigation of individual and group risks.

- **Build trust** by aligning with global data protection best practices, ensuring transparency, obtaining informed consent, and articulating clear exceptions to consent when justified.

- **Advance data security** with strong technical protections, breach mitigation protocols, transparency about data breaches, and consideration of federated data systems.

2. Promote Health Value: To maximize the impact of health data, governance frameworks must enhance health systems, services, and outcomes while supporting innovation.

- **Enhance health systems and services** by using data to improve diagnostics, patient care, and public health monitoring while ensuring benefit flows to contributing communities.

- **Promote data sharing and interoperability** via common standards, multi-sector partnerships, well-defined access levels, and validated consent for data reuse.

- **Facilitate innovation** by integrating emerging technologies responsibly and adapting policies to keep pace with new health data applications and cross-sector data integration.

3. Prioritize Equity: Equity must be embedded in health data governance to ensure fair representation, benefit-sharing, and respect for the rights of all communities.

- **Ensure equitable benefit** by collecting inclusive data, mitigating bias, engaging marginalized communities, and promoting accessible and transparent data use.

- **Establish data rights and ownership** by applying a human rights lens, codifying rights in law, extending those rights to derivative products and services, and ensuring individuals and communities can control and benefit from their data.

- **Define clear roles and responsibilities** for stakeholders and implement participatory mechanisms to ensure long-term, inclusive governance.

- **Connect to broader accountability mechanisms** to integrate health data governance with civic oversight and civil society monitoring efforts.

TRUST Data Principles

Developed by the global data stewardship community and published in 2020, the TRUST Principles for digital repositories provide a framework for ensuring the reliability, integrity, and long-term stewardship of data in open science and research environments (Lin et al., 2020).

T – Transparency

Repository services and the data they host should be easily discoverable and their operations clearly documented. This includes providing clear information about repository policies, governance structures, and data curation practices to foster trust and enable accountability.

R – Responsibility

Repositories must ensure the authenticity and integrity of the data they store. This means implementing processes that verify the accuracy and provenance of datasets and ensuring the persistence and reliability of services over time.

U – User Focus

Repositories should align with the needs and expectations of their designated user communities. This includes engaging users in the development of repository features, metadata standards, and access policies to support usability and relevance.

S – Sustainability

Data and repository services should be maintained over the long term. This principle calls for financial, organizational, and technical strategies to ensure preservation, continuity, and adaptability of data resources.

T – Technology

Repositories should employ robust, secure, and interoperable technologies to support reliable and persistent data access and storage. Technical infrastructure must be regularly updated to meet evolving standards, mitigate risks, and maintain system resilience.

WDS Data Sharing Principles

The **World Data System (WDS) Data Sharing Principles** provide a framework for responsible, ethical, and equitable data sharing to advance research, education, and public good. Developed in alignment with global initiatives such as the Group on Earth Observations, the G8 Open Data Charter, the OECD Principles, and the Science International Accord on Open Data, these principles reflect a commitment to open science and global collaboration. The WDS operates under the auspices of the International Science Council and its historical partners, including the International Council for Science, the International Social Science Council, the InterAcademy Panel, and the World Academy of Science.

- Data, metadata, products, and information should be fully and openly shared, subject to national or international laws and policies, and in accordance with international standards of ethical research conduct.

- Research, educational, and public-domain data should be made available with minimal delay and either free of charge or at no more than the cost of dissemination, with waivers available for lower-income user communities to support equitable access.

- All data producers, users, and sharers are stewards of data and are responsible for preserving the authenticity, quality, and integrity of data, respecting privacy, and ensuring appropriate citation and acknowledgment.

- Data should be open by default, with ‘sensitive’ or ‘restricted’ designations applied only when justified, and should be shared under the least restrictive conditions possible.

- Data must be handled with integrity, confidentiality, and the security levels requested by data stewards and producers.

- Data and repositories should adhere to best practices in data management and stewardship, including the FAIR (Findable, Accessible, Interoperable, Reusable), TRUST (Transparency, Responsibility, User Focus, Sustainability, Technology), and CARE (Collective Benefit, Authority to Control, Responsibility, Ethics) principles.

References

Carroll, S. R., Herczog, E., Hudson, M., Russell, K., & Stall, S. (2021). Operationalizing the CARE and FAIR Principles for Indigenous data futures. *Scientific Data*, *8*(1), 108. https://doi.org/10.1038/s41597-021-00892-0

Coyle, D., Diepeveen, S., & Wdowin, J. (2020). *The value of data summary report*. The Bennett Institute for Public Policy. https://www.bennettinstitute.cam.ac.uk/publications/value-data-summary-report/

D'Ignazio, C., & Klein, L. F. (2023). *Data feminism*. MIT press.

Lin, D., Crabtree, J., Dillo, I., Downs, R. R., Edmunds, R., Giaretta, D., De Giusti, M., L'Hours, H., Hugo, W., Jenkyns, R., Khodiyar, V., Martone, M. E., Mokrane, M., Navale, V., Petters, J., Sierman, B., Sokolova, D. V., Stockhause, M., & Westbrook, J. (2020). The TRUST Principles for digital repositories. *Scientific Data*, *7*(1), 144. https://doi.org/10.1038/s41597-020-0486-7

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

Wilkinson, M. D., Dumontier, M., Aalbersberg, Ij. J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J.-W., Da Silva Santos, L. B., Bourne, P. E., Bouwman, J., Brookes, A. J., Clark, T., Crosas, M., Dillo, I., Dumon, O., Edmunds, S., Evelo, C. T., Finkers, R., … Mons, B. (2016). The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data*, *3*(1), 160018. https://doi.org/10.1038/sdata.2016.18