



# Annex of Illustrative Examples and Initiatives

## Progress Report of the Working Group on Data Governance at All Levels as Relevant for Development

**Contact:** [cstd-datagov@un.org](mailto:cstd-datagov@un.org)

### Note by the secretariat

This annex compiles illustrative examples and initiatives based on inputs submitted by members and observers of the Working Group on Data Governance in response to calls for input issued in the third quarter of 2025 and the first quarter of 2026, as well as on discussions held during the plenary meetings of the Working Group.

The examples and initiatives illustrate existing approaches, frameworks and arrangements relevant to the four substantive chapters of the report. They are non-exhaustive, and their inclusion does not imply endorsement by the Working Group as a whole or by the secretariat. Where an example is relevant to more than one chapter, it may be presented under each relevant chapter from the corresponding perspective, with cross-references where appropriate.



## Chapter 1 – Fundamental principles of data governance at all levels as relevant for development

The following examples and initiatives illustrate different approaches to data governance principles at the national, regional, international and sectoral levels. Section E brings together approaches that relate specifically to data sovereignty, regulatory autonomy and responsible data stewardship.

### A. National and subnational examples

- **Brazil: Brazilian Internet Steering Committee (CGI.br) Principles for the Governance and Use of the Internet** – Provide a rights-based, democratic and multi-stakeholder normative framework relevant to data governance.
- **China: Cybersecurity Law (2017), Data Security Law (2021) and Personal Information Protection Law (2021)** – Establish principles and requirements including data security; classification of data by sensitivity (general, important and core data); risk assessment; explicit and informed consent; data minimization; transparency; and, for transfers abroad, security assessments, standard contracts or certification.
- **Colombia: National Data Infrastructure Plan (PNID)** – Provides a national framework that translates principles such as interoperability, public value generation, accountability and a rights-based approach into institutional capacities, governance models, standards and multilevel arrangements. It is complemented by the Enterprise Architecture Reference Framework (MRAE) and the Interoperability Framework for Digital Government (Marco de Interoperabilidad), which support secure and standardized exchange between public entities.
- **Ecuador: Data governance model for public administration** – Provides a public-sector data governance model aligned with Action 3 of the National Public Integrity Strategy (ENIP), based on legality, quality, integrity from the source and a citizen-focused approach, including the principle that the State should not request information it already holds. Implementation is phased, beginning with entities managing critical data.
- **Estonia: National data strategy** – Sets out governance principles including active transparency on personal data; balancing data availability, data protection and cybersecurity; trust; data quality and standardization; clearly assigned data value; and defined roles, competencies and data literacy. Estonia's experience also illustrates continuing challenges related to standardization and systematic data quality management after extensive use of data exchange systems.
- **Finland: MyData principles** – Set out six guiding commitments: human-centric control of personal data, the individual as the point of integration, individual empowerment, portability, transparency and accountability, and interoperability. Developed in Helsinki in 2014 and subsequently carried forward by MyData Global, they provide an example of an approach aimed at balancing economic and societal uses of data through greater individual agency. Related approaches include the European Union Data Strategy and the MyData law of the Republic of Korea.
- **The Gambia: Data Protection and Privacy Bill 2025 and Access to Information Commission** – Provide an example of the interaction between privacy, access to information and institutional oversight. Relevant elements include data classification, access rules and cross-sectoral oversight, particularly in contexts where enforcement capacity may be constrained.

- **Japan: Data Governance Guidelines (2025)** – Provide a framework for responsible corporate data governance centred on interoperability, trust and value creation. The Guidelines set out four pillars: business processes aligned with cross-border data exchanges, data security, data maturity, and guiding principles for the use of AI and other advanced technologies, while emphasizing executive accountability and continuous improvement in data sharing and utilization.
- **Malaysia (Sarawak): Adat customary law and the Sarawak Biodiversity Centre** – Illustrate approaches to the governance of traditional knowledge. Seven Adat systems have been partially codified and adopted by the courts, while the Sarawak Biodiversity Centre applies free, prior and informed consent and monetary and non-monetary benefit-sharing in research involving traditional knowledge. Digital expressions of Indigenous knowledge remain an area where formal protection is limited.
- **Switzerland: Code of conduct for trustworthy data spaces (Verhaltenskodex für vertrauenswürdige Datenräume)** – Provides a framework for operationalizing digital self-determination and trust through principles including interoperability by default, security, openness and transparency, the once-only principle and federated governance. Related frameworks, including the International Data Spaces Association (IDSA) Reference Architecture Model and the Gaia-X Framework, illustrate approaches combining data sovereignty with interoperability.

## B. Regional examples

- **African Commission on Human and Peoples' Rights: Resolution ACHPR/Res.620 (LXXXI) (2024)** – Affirms access to data in connection with the right to information and illustrates the relationship between data access and the advancement of human rights, while recognizing the need to balance access with other rights (see also chapter 2).
- **African Union and West African Economic and Monetary Union (UEMOA): African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention, 2014) and UEMOA data governance framework** – Provide regional frameworks for personal data protection and data governance in Africa, with relevance for the development and alignment of national and regional approaches (see also chapter 4).
- **European Union: Data Governance Act, Data Act, Open Data Directive, Free Flow of Non-Personal Data Regulation and common European data spaces** – Provide a legal and institutional framework for data sharing and reuse, complemented by common European data spaces and sector-specific rules (see also chapter 4).
- **Council of Europe: Convention 108+ (2018)** – Provides a legally binding framework for data protection that is open to accession by States outside Europe, supporting cross-border safeguards and accountability. Its amending Protocol (CETS No. 223) further modernizes the Convention's data protection framework (see also chapter 4).
- **Asia-Pacific Economic Cooperation (APEC): Cross-Border Privacy Rules (CBPR) System** – Provides a voluntary, accountability-based certification mechanism for cross-border data transfers. The Global CBPR Forum and its Privacy Framework have subsequently built on this approach and are open to participation beyond APEC economies (see also chapter 4).
- **BRICS: Understanding on Data Economy Governance** – Sets out principles including sovereign data governance; fair and equitable access; interoperability and standardization; transparency and accountability; people-centred digital transformation, including digital

public infrastructure (DPI); and shared benefits for inclusive development. Related BRICS instruments include the Joint Declaration of the 15th BRICS Trade Ministers' Meeting and the BRICS Leaders' Statement on the Global Governance of Artificial Intelligence.

### C. International examples

- **International law and human rights instruments: Charter of the United Nations, Universal Declaration of Human Rights and International Covenant on Civil and Political Rights** – Provide foundational international legal and human rights frameworks relevant to data governance, including the protection of rights and consideration of State sovereignty, non-interference and regulatory diversity.
- **FAIR principles (Findable, Accessible, Interoperable, Reusable)** – Provide a widely used reference for the governance and management of scientific, research and public data. They are often considered alongside the CARE and TRUST principles, including to ensure that greater openness and reuse are balanced with collective rights and responsibilities.
- **CARE Principles for Indigenous Data Governance (Collective Benefit, Authority to Control, Responsibility and Ethics)** – Provide a framework for Indigenous data governance grounded in collective rights and responsibilities. They complement the FAIR principles by emphasizing collective benefit, authority to control, responsibility and ethics.
- **Organisation for Economic Co-operation and Development (OECD): Recommendation of the Council on Enhancing Access to and Sharing of Data, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and Declaration on Government Access to Personal Data Held by Private Sector Entities** – Provide policy frameworks relevant to data access, sharing, privacy and cross-border data flows. The Declaration addresses access by public authorities to personal data held by private-sector entities, including considerations related to privacy, proportionality and transparency.
- **United Nations system: Secretary-General's Data Strategy, data principles of the United Nations System Chief Executives Board for Coordination (CEB) and UNCTAD Data Principles for Development** – Provide people-centred frameworks emphasizing value, trust, ethical use and interoperability, with links to human rights and development considerations.
- **UNESCO: Recommendation on the Ethics of Artificial Intelligence (2021)** – Provides a global standard-setting framework on the ethics of artificial intelligence, including a dedicated policy area on data governance. It highlights fairness and non-discrimination, privacy and data protection, safety and security, and transparency and explainability.
- **UNESCO: Convention on the Protection and Promotion of the Diversity of Cultural Expressions (2005)** – Provides an international framework relevant to the protection and promotion of cultural and linguistic diversity, with potential relevance to questions of representation and diversity in data governance and artificial intelligence.
- **Broadband Commission for Sustainable Development: Data Governance in the Digital Age toolkit (July 2025)** – Provides a toolkit for data governance developed under the co-chairship of UNESCO, the International Telecommunication Union (ITU), the United Nations Development Programme (UNDP) and the African Union. It organizes data governance principles around processes, decisions and data handling.
- **Internet Engineering Task Force (IETF) and Internet Architecture Board (IAB): RFC 1958, RFC 1984 and RFC 7258** – Set out architectural and technical principles relevant to an open, interoperable and resilient Internet, including end-to-end design, encryption

and protection against pervasive monitoring.

- **Feminist Data Principles** – Provide a perspective on data governance that highlights power imbalances, bias, lived experience and invisible labour, and the implications of these factors for the collection, use and governance of data.

#### D. Sector-specific examples

- **Official statistics: Fundamental Principles of Official Statistics and European Statistics Code of Practice** – Provide principles and standards for the production, governance and quality of official statistics, including professional independence, impartiality, transparency and protection of statistical confidentiality.
- **Official statistics: Generic Statistical Business Process Model (GSBPM)** – Provides a standardized framework for describing and managing the processes involved in producing official statistics.
- **Official statistics: ESCAP data governance framework and Committee for the Coordination of Statistical Activities (Pathways to Progress)** – Provide broader approaches to data governance across the statistical system. The ESCAP five-pillar framework supports the development of national data governance profiles, while *Pathways to Progress* identifies value, trust and equity as overarching goals across the data life cycle and at international, national and organizational levels.
- **Humanitarian action: Inter-Agency Standing Committee (IASC) Principles for Data Responsibility, Office for the Coordination of Humanitarian Affairs (OCHA) Data Responsibility Guidelines and International Committee of the Red Cross (ICRC) Handbook on Data Protection in Humanitarian Action** – Provide rights-based approaches to responsible data management in humanitarian contexts, including the principle of “do no harm”, protection of affected populations and responsible handling of sensitive data.
- **Children’s data: United Nations Children’s Fund (UNICEF) Responsible Data for Children (RD4C) principles** – Provide a framework for responsible data governance involving children, taking into account their particular vulnerability, limited capacity to provide informed consent and the potential for long-term harm arising from misuse of data.
- **Indigenous data: IEEE 2890-2025 Recommended Practice for Provenance of Indigenous Peoples’ Data** – Provides a framework for the provenance and governance of Indigenous data, emphasizing Indigenous rights, authority and culturally appropriate data practices.
- **Indigenous data: National and community frameworks in Australia, Canada and New Zealand** – Include OCAP® (First Nations, Canada), Tuia te Korowai o Hine Raraunga (Aotearoa New Zealand), Maiam nayri Wingara and the Australian Government’s Framework for the Governance of Indigenous Data (2023), which provide rights-based and community-centred approaches to Indigenous data governance.
- **Health: WHO Data Principles (2021) and WHO Genomic Data Principles** – Provide international principles for responsible governance and use of health and genomic data, including considerations relating to public benefit, trust and responsible data sharing.
- **Health: Health Data Governance Principles (Transform Health)** – Provide a principles-based framework for equitable, rights-based and responsible governance of health data.
- **Health: African Union One Health Information Policy and Architecture, African Digital Health Governance Framework and Cameroon’s One Health data governance framework** – Provide regional and national approaches to health data governance and

exchange in Africa. The African Union One Health Information Policy and Architecture also underpins the African Union Digital One Health Platform and its integrated data contracts.

- **Humanistic Buddhism Centre, Nan Tien Institute: Buddhist Data Principles (2026)** – Provide a values-based approach to data governance emphasizing ethical stewardship, shared responsibility and individual and collective well-being. The principles highlight the role of digital literacy and practical digital ethics in strengthening attention, intention and individual agency, alongside broader safeguards for responsible data use.
- **Agriculture and food systems: Farmer-centric data governance principles** – Provide an approach to data governance that recognizes the particular characteristics of farm data, including the interaction between personal and non-personal data. Key elements include participation of producers and workers, consideration of collective rights relating to land and natural resources, and rights relating to data access, portability and erasure.
- **Research data: TRUST principles and CoreTrustSeal requirements** – Provide frameworks for trustworthy stewardship, preservation and reuse of research data. CoreTrustSeal translates the FAIR and TRUST principles into repository-level requirements.
- **Research data: UNESCO Recommendation on Science and Scientific Researchers (2017) and World Data System practices** – Support long-term access, preservation and responsible stewardship of research data, including through retention and preservation policies.
- **Data management practice: DAMA Data Management Body of Knowledge (DAMA-DMBOK)** – Provides a widely used technical reference for data management practices and governance. It has also been adopted by Peru's National Council for Science, Technology and Technological Innovation (CONCYTEC) as a principal technical reference.

## E. Approaches specific to data sovereignty

The inputs reflect a range of approaches to data sovereignty, including explicitly sovereignty-based frameworks as well as approaches framed in terms of regulatory autonomy, trusted data flows and responsible stewardship.

- **Brazil: General Data Protection Law (Lei Geral de Proteção de Dados, LGPD)** – Provides a rights-based framework centred on privacy, data protection and individual autonomy, supported by strong data subject rights and clearly defined legal bases for data processing. The broader Brazilian approach also links data governance with domestic digital capabilities, public-interest governance and economic development, including through digital public infrastructure such as gov.br and Pix.
- **African Union: African Union Data Policy Framework<sup>1</sup> (2022)** – Provides a sovereignty-based approach focused on strengthening the capacity of African countries to govern their data, derive value from data and participate effectively in regional and global data flows. It also emphasizes protection against extractive practices, collective and communal interests, and equitable value creation.
- **European Union: Data Union Strategy, Pillar III<sup>2</sup>** – Frames data sovereignty in terms of Europe's capacity to retain control over how data are accessed, used and protected within and beyond its borders. This approach is presented as compatible with openness to trusted

<sup>1</sup> African Union, African Union Data Policy Framework (Addis Ababa, 2022).

<sup>2</sup> EU Data Union Strategy, Unlocking Data for AI, Pillar III: Safeguarding the EU's data sovereignty through a strategic international data policy, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0835>.

partners where data exchanges are fair, secure and consistent with EU laws, values and strategic interests.

- **Association of Southeast Asian Nations (ASEAN)** – Emphasizes trusted cross-border data flows, interoperability and regulatory autonomy rather than explicitly using the language of data sovereignty. These approaches are intended to support innovation, digital trade and regional and international cooperation.
- **Southern Common Market (MERCOSUR) and Economic Commission for Latin America and the Caribbean (ECLAC)** – Illustrate regional approaches that link data governance with accountability, rights, development, economic inclusion, innovation and strategic autonomy.
- **OECD: Data Free Flow with Trust (DFFT)** – Provides an approach aimed at reconciling cross-border data flows with legitimate public policy objectives, including privacy, security and trust. It illustrates how openness to data flows can coexist with regulatory autonomy and other considerations associated with data sovereignty.
- **ISO/IEC 38505-1:2026, Governance of data<sup>3</sup>** – Provides an international standard for the governance of data based on responsible, accountable and inclusive practices. While not framed explicitly in terms of data sovereignty, it emphasizes ethical and culturally respectful data handling, protection of stakeholder rights and responsible stewardship of organizational and public-sector data, including attention to Indigenous Peoples' data.
- **IEEE 2890-2025, Recommended Practice for Provenance of Indigenous Peoples' Data** – Provides a framework for Indigenous data governance and provenance, including recognition of Indigenous Peoples' authority over the collection, ownership and use of their data. It supports the incorporation of Indigenous perspectives on data governance and provenance within broader frameworks.

---

<sup>3</sup> International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 38505-1:2026: <https://www.iso.org/standard/87195.html>.

## Chapter 2 – Considerations of sharing the benefits of data

The following examples and initiatives illustrate different approaches to sharing the benefits of data. They include arrangements that support data access and use, capacity-building and equitable participation in the data economy at the national, regional and international levels and across specific sectors.

### A. National and subnational examples

- **Brazil: gov.br, Pix and Conecta gov.br** – Provide digital public infrastructure on which innovative services can be developed. Through Conecta gov.br, public agencies can integrate curated data shared via application programming interfaces (APIs), supporting more efficient public services and reuse of government data.
- **China: Plan to Promote Common Prosperity through the Digital Economy (December 2023) and Interim Provisions on Accounting Treatment of Enterprise Data Resources (August 2023)** – Illustrate approaches to linking the use and valuation of data with broader development objectives. The Plan emphasizes the role of the digital economy in narrowing regional gaps, while the Interim Provisions incorporate data resources into enterprise accounting systems. Related development funds and tax incentives support public welfare and the digital transformation of small and medium-sized enterprises (SMEs).
- **China: Chongqing Integrated and Smart Public Data Platform** – Provides a municipal platform for aggregating and managing public data across departments and different levels of government. It supports secure data circulation and use across sectors including urban safety, health care, automotive manufacturing and logistics.
- **China: Shanghai One-Stop Service Platform and Unified Urban Management Platform** – Provide digital government infrastructure that streamlines administrative services and supports urban management through citywide data integration, real-time monitoring and risk response.
- **China: Zhejiang Integrated and Intelligent Public Data Platform** – Supports unified public data cataloguing, cross-level data sharing and public service delivery, including simplified administrative procedures through the “Zheliban” service portal.
- **Finland: MyData** – Provides a framework for strengthening individuals’ control over and ability to use data concerning them, including through actionable data rights and the once-only principle. It also illustrates approaches to broadening participation in data ecosystems and reducing dependence on concentrated data infrastructures.
- **The Gambia: Government Open Data Strategy 2024–2027 and National Data Policy 2025** – Provide a national framework for expanding access to and use of data, supported by investment in digital public goods (DPGs) and shared digital infrastructure under the Recovery-Focused National Development Plan 2023–2027. Relevant elements include data-sharing arrangements, local use and accountability mechanisms.
- **India: Aadhaar and Unified Payments Interface (UPI)** – Provide digital public infrastructure that, together with cloud computing and national data exchanges, supports wider access to digital services and inclusive innovation in areas including financial and civic technology.
- **India: Community stewardship model for non-personal data (2020)** – Proposes an approach under which an independent authority could require the sharing of designated

high-value non-personal datasets for public-interest purposes, subject to safeguards including protection of trade secrets.

- **Japan: Cross-sectoral data spaces** – Support data sharing and reuse in sectors including automotive, chemicals and drone navigation. Open-source resources and entry-level services are provided as digital public goods to reduce cost and expertise barriers for SMEs, supported by the Public Interest Digital Platform Operator Certification and institutions such as the Information-technology Promotion Agency (IPA). The Japan AI Safety Institute has also published a freely accessible Data Quality Management Guidebook.
- **Peru: DATOS PERÚ and GEOPERÚ** – Provide cross-cutting platforms for secure and responsible access to government data, including for smaller actors such as SMEs and community groups. They illustrate how DPGs and DPI can broaden access to reliable and high-quality public data.
- **Philippines: Computing and Archiving Research Environment (COARE)** – Provides high-performance computing and cloud infrastructure with free access for students, researchers and analysts, helping broaden access to advanced digital and computational resources.
- **Switzerland: Code of conduct for trustworthy data spaces and Swiss Data Ecosystem (Datenökosystem Schweiz)** – Promote responsible participation in data ecosystems and fair distribution of benefits among stakeholders. The Swiss Data Ecosystem point of contact also supports exchange of experience, learning and good practices among participating actors.
- **United States of America: Federal Risk and Authorization Management Program (FedRAMP)** – Provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services used by the federal government, helping establish trusted conditions for access to and use of cloud-based digital infrastructure.

## B. Regional examples

- **African Commission on Human and Peoples' Rights: Resolution ACHPR/Res.620 (LXXXI) (2024)** – Affirms access to data in connection with the right to information and provides a basis for considering how individuals and communities that generate or contribute data may participate in and benefit from its use.
- **African Union: African Union Data Policy Framework (2022)** – Provides a regional framework for harmonizing data governance and supporting a single digital and data market in Africa. It promotes interoperable and open data, access to public data systems for research, innovation and the public interest, and approaches such as data stewardship and collective privacy rights aimed at ensuring that communities benefit from data use.
- **African Union: African Continental Free Trade Area (AfCFTA)** – Provides a regional framework for cross-border cooperation, technology transfer and participation in the digital economy. Its relevance to data governance includes the development of cross-border data arrangements that can support a more integrated African digital market and wider access to the benefits of data and AI.
- **European Union: Sovereignty Effective Assurance Levels (SEAL)** – Provides a scoring scale developed within the EU Cloud Sovereignty Framework to assess the degree of control, security and digital independence associated with cloud services, technologies

and operations. It supports trusted mechanisms for secure data hosting and cross-border digital services.

### C. International examples

- **International Testbed for Dataspace Technology (ITDT), University of Tokyo** – Provides a research and verification environment for dataspace technologies and supports cross-border coordination among public, private and academic actors.
- **Nwulite Obodo Open Data License** – Provides a licensing approach for African datasets that differentiates between users from Africa and other developing countries and other users. Users outside those regions are subject to equivalent sharing conditions and may be required to provide royalties or other benefits to dataset owners.
- **OECD: Recommendation of the Council on Enhancing Access to and Sharing of Data (2021)** – Encourages approaches that promote fair distribution of the benefits arising from data access and sharing, including through appropriate incentives and capacity-building.
- **United Nations: Governing AI for Humanity (2024) – proposal for a global initiative on AI and data commons** – Presents data commons as governed environments in which data can be pooled for public or collective purposes, providing an approach to broadening access to data and sharing the benefits derived from its use.

### D. Sector-specific examples

- **Health and social protection: DHIS2, openIMIS and SORMAS** – Provide open-source systems for health information management, health financing, social protection, and epidemic surveillance and response. Their open-source design enables local adaptation and wider access to digital infrastructure and services. DHIS2 operates at scale in the health sector, while openIMIS is reported to benefit more than 36 million people in 14 countries.
- **Health: African Union Digital One Health Platform** – Provides an open-source platform for integrating, analysing and visualizing One Health data from member States through decentralized data spaces. Its integrated data contracts establish arrangements between data owners and recipients and support structured data exchange.
- **Health: European Health Data Space** – Provides a framework for access to health data through a data permit system under which requests must meet specified public-value conditions. Where users enrich datasets accessed under a permit, the enriched data are returned to the data pool, supporting wider reuse and circulation of benefits.
- **Health research: China's multicentre health research network** – Links more than 150 institutions across 23 provincial-level regions through a “centralized coordination + distributed custody” model. The network is connected to an innovation centre that has incubated 32 enterprises, illustrating an approach to sharing research, innovation and economic benefits across the data value chain.
- **Agriculture and food systems: Vision Statement on Data for Food Security and Nutrition (October 2023) of the Civil Society and Indigenous Peoples' Mechanism (CSIPM) for relations with the Committee on World Food Security (CFS)** – Provides a rights-based perspective on food and agricultural data, emphasizing the interests of Indigenous Peoples, women, peasants, food workers and consumers. It also highlights questions concerning how value generated through agricultural data is distributed across data ecosystems.

- **Agriculture: Wushan County Crisp Plum “Industrial Brain”, China** – Uses data as a factor of production to improve agricultural management and address development constraints in fruit growing. The initiative is reported to have increased output value per mu in 2024 and contributed to higher incomes for fruit-growing households.
- **Environmental and territorial monitoring: Community-generated data in the Brazilian Amazon** – Illustrate how community-led and Indigenous-led data initiatives can combine locally generated information with digital tools to monitor socio-environmental conditions, defend territories and support the protection of local and Indigenous communities.
- **Biodiversity and traditional knowledge: Sarawak Biodiversity Centre, Malaysia** – Provides a governance framework for research involving traditional knowledge associated with biological resources, including arrangements relevant to access, consent and benefit-sharing.
- **Biodiversity: Access and benefit-sharing arrangements under the Convention on Biological Diversity** – Provide mechanisms for sharing monetary and non-monetary benefits arising from the use of biological resources and associated knowledge, including with Indigenous Peoples and local communities. More recent arrangements relating to digital sequence information also provide a model for multilateral benefit-sharing linked to the use of data-derived resources.
- **Indigenous data: CARE principles, free, prior and informed consent (FPIC) and access and benefit-sharing (ABS) practices** – Provide rights-based approaches to the governance of Indigenous data, emphasizing collective benefit, authority to control, responsibility and ethics, alongside consent and benefit-sharing arrangements.
- **Indigenous data and cultural heritage: Australia’s Framework for the Governance of Indigenous Data (National Indigenous Australians Agency, 2023) and Yirrkala Literature Production Centre** – Illustrate approaches in which Indigenous governance is embedded in the collection, curation, storage and access to data and cultural materials. The Yirrkala Literature Production Centre combines community-directed access, governance-visible cataloguing and secure storage on Yolŋu Country.
- **Research: Peru’s National Current Research Information System (PeruCRIS) and open access to publicly funded research data** – Provides infrastructure that allows smaller universities and individual researchers to manage and make research outputs more visible without requiring costly proprietary systems. Open-access approaches to publicly funded research data can further broaden access to and reuse of research results.
- **Civil registration and geospatial data: OpenCRVS and OpenStreetMap** – Provide open-source and openly accessible digital resources that can be adapted locally and used by start-ups, local governments and civil society to develop services and applications.
- **Disaster risk management: GeoRisk Philippines** – Provides a government-led, multi-agency platform for accessing information on natural hazards and risk assessment, supporting wider use of public data for disaster preparedness and decision-making.
- **Language and linguistic diversity: Mozilla Common Voice** – Provides a community-based, open-access repository of voice data in which individuals can contribute, validate and use datasets, with particular attention to under-represented languages.
- **Logistics and trade: China–Europe Railway Express (Xi’an) Data Information Platform** – Supports cross-border trade and logistics through data interconnection and integrated digital services, including customs declaration, booking, electronic contracts, shipment tracking, payments and supply-chain services. The platform illustrates how data

sharing can reduce administrative burdens and improve operational efficiency.

- **Financial services: Shenzhen–Singapore Cross-Border Data Validation Platform (China and Singapore)** – Provides a cross-border data validation arrangement supporting financing and international business development. Its pilot use case uses credit information reports of business owners to facilitate access to cross-border financing for SMEs.

## Chapter 3 – Proposals to support interoperability between national, regional and international data systems

The following examples and initiatives illustrate national, regional and sectoral arrangements, as well as international standards, that support interoperability between data systems.

### A. National and subnational examples

- **Brazil: gov.br and Pix** – Provide national digital public infrastructure supporting interoperable public and financial services. gov.br is underpinned by Conecta gov.br, which enables data sharing between public agencies through application programming interfaces (APIs) and supports the once-only principle. Pix is an interoperable instant payment infrastructure operated and regulated by the Central Bank of Brazil, based on open standards and multi-stakeholder governance.
- **China: National Data Infrastructure Construction Guidelines** – Provide for a national data infrastructure based on distributed data directories, distributed digital identity and standardized interfaces, supporting data exchange and interoperability across systems and jurisdictions.
- **China: Trustworthy data spaces** – Provide five types of data spaces—enterprise, city, cross-border, industry and personal—serving as multi-level components of the national integrated data market. They support compliant data circulation, value creation and protection of rights and security across different use cases.
- **Colombia: Interoperability Framework for Digital Government (Marco de Interoperabilidad)** – Provides principles, recommendations and technical guidance for secure and efficient information exchange between public entities, including the Common Language for Information Exchange as a national standard for interoperability.
- **Estonia: X-Road** – Provides a federated data exchange layer that enables secure and interoperable information exchange across public and private systems. The model has also been adapted and implemented in other countries, including developing economies.
- **India: Aadhaar and Modular Open Source Identity Platform (MOSIP)** – Provide digital identity infrastructure supporting interoperable public and digital services. Aadhaar is India's foundational digital identity system, while MOSIP provides an open-source and modular identity platform that can be adapted by other countries.
- **Indonesia: Satu Data Indonesia (One Data Indonesia)** – Provides a whole-of-government framework for data standards, metadata, interoperability, reference codes, master data and institutional roles. It is supported by the data.go.id portal, the National Data Catalogue and Data Insight dashboards managed by the Ministry of National Development Planning (Bappenas).
- **Japan: Infrastructure for Multi-layer Interoperability (IMI)** – Provides a structured approach to semantic interoperability through hierarchical core vocabularies and data models designed to align with international standards while preserving local meaning.
- **Japan: Ouranos Ecosystem and Open Data Spaces** – Provide data-sharing architectures for manufacturing and utility sectors, aimed at facilitating interoperable data exchange and reducing technical and cost barriers to participation, including for SMEs along supply chains.
- **Peru: State Interoperability Platform (PIDE)** – Provides the legal and technical

infrastructure for secure government-to-government data exchange and interoperability.

- **Portugal: National interoperability platforms** – Provide interoperability infrastructure across public administration and sectoral systems, including social security, life sciences and health, and integrated rural fire management.
- **Switzerland: Swiss Data Ecosystem (Datenökosystem Schweiz) principles** – Provide a national framework for trusted data ecosystems based on interoperability, digital self-determination and responsible data sharing.
- **Switzerland: TERMDAT** – Provides a multilingual terminology database that supports semantic interoperability across Switzerland's language regions and public administration.

## B. Regional examples

- **African Union: Common Data Categorisation and Sharing Framework** – Provides a regional approach to data categorisation and sharing under the African Union Data Policy Framework, supporting greater consistency and interoperability across national data ecosystems.
- **European Union: European Interoperability Framework (EIF)** – Provides a common framework for legal, organizational, semantic and technical interoperability and supports the development of national interoperability frameworks across EU member States.
- **European Union: Interoperability regulatory sandboxes under the Interoperable Europe Act** – Provide controlled environments for testing new technological and organizational solutions to interoperability while supporting collaboration and maintaining applicable legal and governance safeguards.

## C. International standards supporting interoperability for development

The following international standards provide technical and architectural references relevant to interoperability across data systems, platforms and infrastructures:

- **ITU-T Y.3600 (11/2015), Big data – Cloud computing based requirements and capabilities** – Provides requirements and capabilities for cloud-based big data systems and related interoperability.
- **ISO/IEC/IEEE 42010:2022, Software, systems and enterprise – Architecture description** – Provides principles and requirements for describing system and enterprise architectures in a consistent and interoperable manner.
- **IEEE 3800-2024, Standard for a Data-Trading System: Overview, Terminology and Reference Model** – Provides common terminology and a reference model for data-trading systems.
- **IEEE 2413-2019, Standard for an Architectural Framework for the Internet of Things (IoT)** – Provides an architectural framework for IoT systems, supporting interoperability across applications, platforms and sectors.
- **ISO/IEC 11179-1:2023, Information technology – Metadata registries (MDR) – Part 1: Framework** – Provides a framework for metadata registries that supports consistent data definitions and semantic interoperability.
- **ISO 8000-1:2022, Data quality – Part 1: Overview** – Provides foundational concepts and principles for data quality, supporting reliable and interoperable data exchange.

## D. Sector-specific examples

- **Health classifications and standards: International Classification of Diseases, 11th Revision (ICD-11) and WHO Family of International Classifications** – Provide standardized classifications and common terminology that support consistent recording, comparison and exchange of health information across countries and health systems.
- **Health data exchange and platforms: DHIS2; African Union One Health Information Policy and Architecture; and African Union Digital One Health Platform** – Provide operational approaches to interoperable health data management and exchange. DHIS2 is an open-source digital public good that combines common core components with local adaptation, while the African Union Digital One Health Platform supports integration of One Health data from member States through decentralized data spaces and data contracts defining what data are shared and for which purposes.
- **Identity and inclusion: Interoperability between humanitarian registration systems and national civil registration and identity systems** – Can support access to services and inclusion for refugees, stateless persons and internally displaced persons, where appropriate safeguards and clearly defined purposes are in place. Such interoperability also requires careful governance because identity data can enable persistent linkage across systems and may create risks of exclusion, discrimination or surveillance.
- **Meteorology: Cross-border exchange of observational data** – Supported through the World Meteorological Organization (WMO) Unified Data Policy, enabling international exchange of meteorological and related observational data for purposes including early warning, disaster response and monitoring of transboundary resources.
- **Ocean data: Ocean Data and Information System (ODIS)** – Provides an interoperable and federated system for ocean data and metadata exchange, developed under the United Nations Decade of Ocean Science for Sustainable Development and based on schema.org.
- **Seismic data: Standard for the Exchange of Earthquake Data (SEED)** – Provides a standardized protocol for the exchange of continuous seismic data among geophysical institutions, supporting early warning, scientific collaboration and data sharing across borders.
- **Spatial data infrastructure: Infrastructure for Spatial Information in the European Community (INSPIRE)** – Provides a common framework for spatial data infrastructure in the European Union, supporting interoperability and access to environmental and geospatial data across jurisdictions.
- **Science, technology and innovation policy: UNESCO Global Observatory of Science, Technology and Innovation Policy Instruments (GO-SPIN)** – Provides a standardized methodology for monitoring science, technology and innovation policies across countries, while supporting national ownership of data and related capacity-building.

## Chapter 4 – Options to facilitate safe, secure and trusted data flows, including cross-border data flows as relevant for development

The following examples and initiatives illustrate national, regional, international and sectoral options to facilitate safe, secure and trusted data flows, including cross-border data flows.

### A. National and subnational examples

- **Brazil: General Data Protection Law (LGPD)** – Provides mechanisms for lawful cross-border transfers of personal data, including adequacy decisions, standard contractual clauses and binding corporate rules, alongside safeguards for the protection of personal data transferred abroad.
- **China: Cross-border data validation platform** – Provides a technical mechanism for cross-border data verification while allowing raw data to remain within the respective jurisdictions. Using the Distributed Data Transfer Protocol (DDTP) and blockchain technology, the platform exchanges hash values for verification and has been applied in Shenzhen–Hong Kong, China and Shenzhen–Singapore use cases, including to support cross-border financing for SMEs.
- **China: Regulations on Promoting and Regulating Cross-Border Data Flows and Measures for the Certification of Personal Information Protection for Cross-Border Data Transfers** – Provide regulatory mechanisms for lawful and orderly cross-border data transfers, seeking to facilitate data flows while maintaining requirements relating to data security and personal information protection.
- **Colombia: National Data Infrastructure Plan (PNID) and data governance model (MGID)** – Provide a national framework supporting secure and governed data exchange, including institutional, technical and governance arrangements for sharing data across public and private actors.
- **Egypt: Personal Data Protection Law and its Executive Regulation** – Establish requirements for the processing, security and cross-border transfer of personal data. The framework combines safeguards for data transferred abroad with a risk-based approach under which more sensitive or critical data may be subject to stronger restrictions, while less sensitive data can circulate under applicable protections.
- **United Kingdom of Great Britain and Northern Ireland: Data (Use and Access) Act 2025** – Provides a legal framework for international transfers of personal data, supported by transfer mechanisms including the International Data Transfer Agreement (IDTA) and binding corporate rules.

### B. Regional examples

- **African Union: African Union Data Policy Framework (2022)** – Provides a regional policy framework for data governance that emphasizes developmental use of data, public-interest regulation and approaches to cross-border data flows that take account of differences in digital readiness, data maturity and national regulatory environments.
- **African Union: African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)** – Provides a continental legal framework for data protection and cybersecurity and supports greater harmonization of national laws relevant to cross-border data flows.
- **Asia-Pacific Economic Cooperation: Cross-Border Privacy Rules (CBPR) System** –

Provides a voluntary, accountability-based mechanism for facilitating cross-border transfers of personal data among participating economies while maintaining privacy protections.

- **Association of Southeast Asian Nations: ASEAN Framework on Digital Data Governance and ASEAN Model Contractual Clauses** – Provide complementary regional mechanisms for cross-border data flows. The Framework promotes greater business certainty and seeks to avoid unnecessary restrictions on data transfers, while the Model Contractual Clauses provide standardized legal terms for transfers between organizations.
- **Economic and Social Commission for Asia and the Pacific: Project “Advancing cross-border data sharing platform in pilot countries with a focus on digital public services” (2023–2026)** – Supports the development and testing of cross-border data-sharing arrangements for digital public services, including through pilot work with Kazakhstan, the Republic of Korea and Uzbekistan.
- **Economic and Social Commission for Asia and the Pacific: Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific** – Provides a regional platform for developing and testing legal and technical solutions for electronic data exchange and cross-border mutual recognition in paperless trade.
- **European Union: General Data Protection Regulation (GDPR)** – Provides mechanisms for international transfers of personal data, including adequacy decisions, standard contractual clauses and binding corporate rules.
- **European Union: Free Flow of Non-Personal Data Regulation** – Supports the movement of non-personal data within the European Union by restricting unjustified data localization requirements.
- **European Union: Data Act and Data Governance Act** – Provide complementary frameworks for data access, sharing and reuse across sectors and borders, while establishing safeguards and governance arrangements for trusted data use.
- **European Union: Common European data spaces** – Provide sectoral environments for trusted data sharing that combine technical infrastructure with governance arrangements and operate in accordance with applicable EU data protection and data governance rules.

### C. International and plurilateral mechanisms for trusted data flows

- **Council of Europe: Convention 108+** – Provides a legally binding framework for data protection that supports cross-border data flows through common safeguards, accountability requirements and protections for personal data among its Parties.
- **Data Free Flow with Trust (DFFT)** – Provides an international approach to facilitating cross-border data flows while maintaining trust through safeguards relating to privacy, security and intellectual property. First proposed by Japan in 2019 and endorsed by the Group of 20 (G20) at the Osaka Summit, the approach is being further operationalized through international cooperation, including at the OECD.
- **Global Cross-Border Privacy Rules (CBPR) Forum: Global CBPR System and Global Privacy Recognition for Processors (PRP) System** – Provide international certification mechanisms aimed at supporting trusted cross-border transfers of personal data through common privacy and accountability requirements.
- **Global Cross-border Data Flow Cooperation Initiative (China, November 2024)** – Sets out principles for cross-border data flows based on openness, inclusiveness, security,

cooperation and non-discrimination, while emphasizing support for developing and least developed countries to participate effectively in the global data economy.

- **IETF and IAB: RFC 1958, RFC 1984, RFC 7258 and RFC 7754, and related IAB statements** – Provide technical and architectural principles relevant to an open, interoperable and resilient Internet, including the role of end-to-end encryption and protection against pervasive monitoring in supporting trusted data exchange across borders.
- **ISO/IEC 27001 and ISO/IEC 27701** – Provide international standards for information security management and privacy information management, supporting secure, accountable and traceable handling of data across organizations and jurisdictions.
- **OECD: Declaration on Government Access to Personal Data Held by Private Sector Entities (2022)** – Sets out common principles for government access to personal data held by private-sector entities for law enforcement and national security purposes, with the aim of strengthening safeguards, accountability and trust in cross-border data flows.

#### D. Sector-specific examples

- **Health: WHO Global Digital Health Certification Network (GDHCN)** – Provides an interoperable trust architecture that enables WHO member States to verify the authenticity of digital health records and certificates across borders through shared software infrastructure.
- **Health: African Union One Health Information Policy and Architecture and African Union Digital One Health Platform** – Provide a regional framework and technical platform for the exchange and use of One Health data across African countries and sectors. The Digital One Health Platform integrates data from member States through decentralized data spaces and uses data contracts to define what data are shared, how frequently and for what purposes.
- **Meteorology: WMO Unified Data Policy, WMO Information System 2.0 (WIS 2.0) and World Weather Watch** – Provide international frameworks and infrastructure for the exchange of meteorological, climate and disaster-related data. They support standardized and open data sharing across countries, including through technical assistance and equipment support for developing countries.
- **Seismology: Standard for the Exchange of Earthquake Data (SEED)** – Provides a standardized protocol for the exchange of seismic data among geophysical institutions, supporting cross-border scientific cooperation and early-warning functions.
- **Humanitarian and displacement statistics: Office of the United Nations High Commissioner for Refugees (UNHCR) statistics and Statistical Quality Assurance Framework for Official Statistics (SQAF)** – Support the collection, integration and responsible sharing of data on forcibly displaced and stateless populations. The SQAF provides quality standards and statistical disclosure controls to reduce the risk of identifying individuals in shared data.
- **Environment: Amazon Basin Project of the Amazon Cooperation Treaty Organization, the United Nations Environment Programme and the Global Environment Facility** – Supports cross-border pooling and sharing of environmental data among Amazonian countries, facilitating regional cooperation, environmental monitoring and coordinated governance.