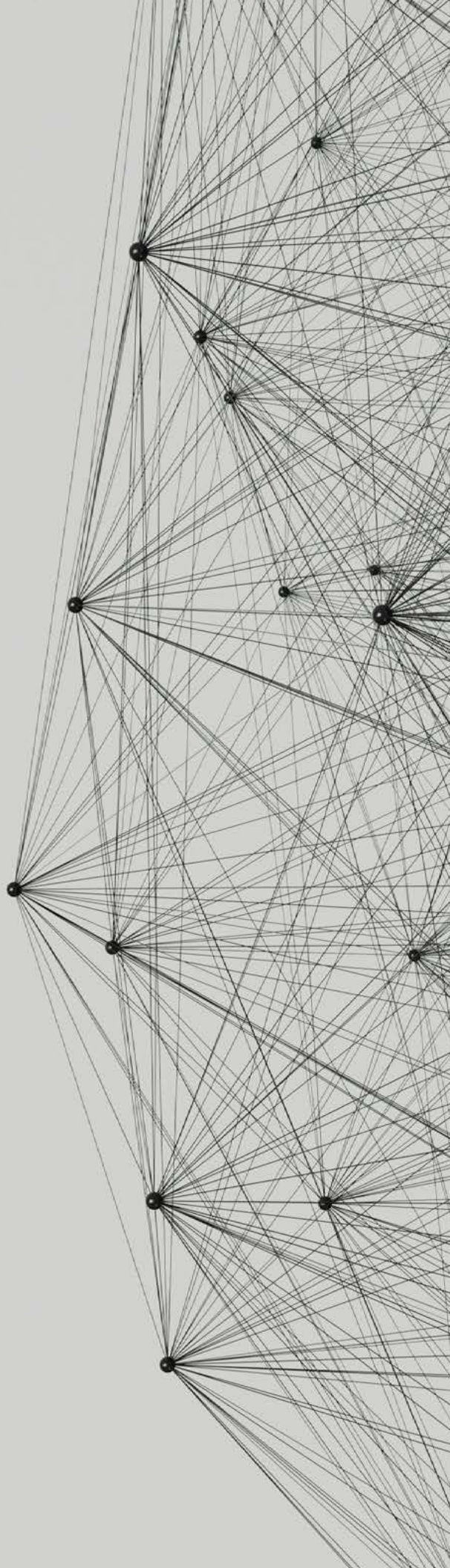
FEBRUARY 2026

WHAT IS DATA GOVERNANCE: 30 QUESTIONS AND ANSWERS

A practical reference for policy, institutional, and operational design

Stefaan Verhulst, Begoña G. Otero



GOVLAB

Table of Contents

Introduction and Purpose of this Q&A

This document is designed as a practical reference that can be read end-to-end—as a structured primer on data governance—or used modularly to support workshops, institutional design, policy drafting, and capacity-building. The Q&A is intentionally organized into a small number of thematic blocks, moving from foundational definitions and conceptual boundaries, through purpose and principles, people, practices, implementation and accountability, and emerging directions.

The structure serves three functions. First, it establishes a shared vocabulary and clarifies distinctions between concepts that are frequently conflated, such as governance, strategy, ethics, privacy, and management. Second, it foregrounds the normative design choices that shape data governance outcomes in practice—particularly questions of purpose, principles, legitimacy, and stewardship. Third, it situates data governance within real institutional, technical, sectoral, and cross-border contexts, recognizing that what is feasible depends on capacity, architecture, and scale.

The Q&A aligns with the working definition of the *Data Governance Toolkit: Navigating Data in the Digital Age*, developed under the Broadband Commission for Sustainable Development Working Group on Data Governance (chaired by UNESCO and co-chaired by ITU, UNDP, and the African Union). Consistent with that approach, data governance is treated not merely as compliance or control, but as purpose-driven, principles-based, and stewardship-oriented decision-making across the data lifecycle. It explicitly links governance to agency and participation (including agency-oriented principles such as Digital Self-Determination (DSD)), to social licensing as a pathway to legitimacy, and to a critical engagement with technological determinism—where technical design choices risk becoming de facto governance unless they are deliberately governed.

Section I.

Foundations and Scope

1. What is data governance?

Data Governance involves ***the processes, people, policies, practices and technology*** *that seek to govern* ***the data lifecycle*** *toward meeting the* ***purpose*** *of increasing trust, value, and equity, while minimizing risk and harm in alignment with a set of* ***core principles***.

As such, when defining a data governance framework, four key elements and activities need to be specified:

- ***Why:*** Defining the vision and purpose for data and data governance.
- ***How:*** Specifying the principles that will guide and determine how decisions are made and practices implemented to meet the purpose responsibly and effectively.
- ***Who:*** Establishing processes and engaging people necessary to create and enforce policies and practices that can meet the purpose in alignment with the principles.
- ***What:*** Specifying and implementing the policies, practices and technologies that govern the different stages of the data lifecycle, in ways that meet the purpose and comply with the principles.

2. Why is it important?

Data is a vital resource for digital innovation and decision-making. Generally, data governance involves guiding how data should be generated and (re)used. Depending on the actor, data governance can signify different things. For businesses, the term is often used to describe internal governance arrangements that enable value creation and compliance. For states, data governance should relate to policies concerning the generation and (re) use of data in various contexts to promote the attainment of public interest goals.

Overall, data governance:

- Encompasses the overall framework for how data is governed, including principles, processes, policies, and practices that aim to generate value from data while minimizing harm.
- It is about ensuring that data is governed throughout its lifecycle, balancing both protection and access for reuse.
- Definitions and instruments of data governance vary by jurisdiction. Some countries may turn to the judiciary for guidance; others may rely on political or constitutional definitions and protections.

3. Is data governance the same as a data strategy?

No. Data governance guides how data is generated and (re)used, ensuring proper management for businesses or public interest goals. Data strategy defines how data is leveraged to create value and achieve objectives. Governance sets the framework; strategy drives its use.

4. How does data governance differ from data management?

Data governance guides how data should be generated and (re)used, ensuring proper management for businesses or public interest goals. Data management focuses on the technical and operational processes of, for instance, storing, processing, and accessing data.

5. Is data governance the same as data ethics?

No, but they are closely related. Data governance guides how data should be generated and used, ensuring it is managed effectively for business or public-interest goals. Data ethics focuses on the responsible and fair use of data, addressing issues like privacy, bias, and societal impact. Strong data governance can support ethical data use, but ethics go beyond governance to consider broader moral implications.

Overall, data ethics:

- Relates to the principles and values guiding how data should be used, especially concerning human rights, fairness, accountability, transparency, and social impact.
- It involves making moral judgments on what is considered acceptable or unacceptable use of data, aiming to prevent harm to human rights and promote societal good.
- There may be instances where the ethics of using data can take priority over the ethics specified in data governance regulations. Data governance rules here would constitute a floor, while ethics in application would constitute a ceiling.
- Views on data ethics may differ based on culture, religion, and upbringing.

6. Is data governance the same as data protection, personal data protection, or data privacy?

No, but they are closely related and often operationally interdependent. Data governance is the umbrella decision-making framework that sets the purpose, principles, roles, processes, and controls for how data is collected, used, shared, and retained across the full data lifecycle (including both protection and responsible access/reuse). Data protection, personal data protection, and data privacy are specific domains within (or adjacent to) that umbrella—each addressing a narrower set of risks, rights, and safeguards.

Data protection is primarily about protecting data (personal or non-personal) against loss, unauthorized access, alteration, or disclosure. It is security focused. It emphasizes technical and organizational safeguards and security governance, such as:

- access controls and authentication,
- encryption and secure storage/transfer,
- anonymization/pseudonymization where appropriate,
- logging, monitoring, incident response,
- audits, breach management, and integrity controls.

In practice, strong data governance *includes* data protection because security is a necessary condition for trustworthy data use—but data protection alone does not define purpose, legitimate reuse pathways, stewardship roles, or broader accountability across the lifecycle.

Personal data protection refers to the legal duties and compliance requirements that apply when processing personal data (e.g., lawfulness, fairness, transparency, purpose limitation, data minimization, security, accountability, and enforceable rights—depending on the jurisdiction). It focuses on:

- who may process personal data and on what legal basis,
- what obligations apply to controllers/processors,
- what rights and remedies individuals have,
- what regulatory oversight and sanctions exist.

Data governance often operationalizes these duties (e.g., assigning roles, embedding controls, creating evidence for compliance), but it is broader than personal-data compliance and can cover governance of non-personal data, interoperability, access arrangements, and reuse for public value.

Data privacy centers on the rights, expectations, and norms that shape how personal information should be collected and used—especially an individual's ability to understand and influence what happens to their data. Privacy typically includes:

- informed participation and meaningful choice (where applicable),
- limits on collection and secondary use,
- transparency and explainability about data use,
- rights such as access, correction, deletion/erasure, portability, and objection (where provided by law),
- contextual sensitivities that can vary across cultures and communities.

Data governance should respect and implement privacy requirements and norms, but privacy by itself does not answer wider governance questions (e.g., how to enable responsible data sharing for public interest, who acts as steward, how to ensure lifecycle traceability, or how to align systems with stated purpose and principles).

In a nutshell, data governance is the system of decision-making and stewardship over data across its lifecycle; data protection is security safeguards; personal data protection is legal compliance for personal data processing; and data privacy is rights and expectations about personal information and autonomy.

7. What's the difference between data governance and AI governance?

Data governance guides how data should be generated and (re)used, ensuring quality, integrity, security, and compliance. AI governance focuses on the development, deployment, and oversight of AI systems, ensuring they operate ethically, transparently, and safely. Data governance is the bedrock of AI governance, as data is the foundation of any AI system.

Section II.

Purpose

8. Why is it important to define a vision and purpose for data and data governance?

A clearly articulated purpose and vision are foundational to any effective data governance strategy. They help answer the 'why' behind data collection, use, sharing, and protection. Without a guiding purpose, data initiatives risk being fragmented, misaligned, or even harmful. Purpose provides direction, coherence, and a basis for accountability across the data lifecycle—from planning and collection to analysis and reuse.

9. What should a purpose for data governance include?

An effective purpose statement should:

- Reflect the organization's core values and societal priorities (e.g., equity, innovation, human rights).
- Be actionable, aligning with policy objectives or strategic goals.
- Address both opportunities (e.g., data reuse, AI enablement) and risks (e.g., harm, exclusion, bias).
- Serve as a benchmark for governance decisions, success indicators, and continuous improvement.

10. What are some common purposes for data governance?

Organizations may define their data governance purpose in terms of one or more of the following:

- Maximizing Data Utility and Value – e.g., data reuse for insights, economic growth.
- Fostering Innovation and Sustainable Development – e.g., AI development, SDG tracking.
- Establishing Equity – e.g., inclusive data practices.
- Supporting Specific Policy or Operational Objectives – e.g., transparency, crisis response, health outcomes.
- Advancing Agency and Participation – e.g., Digital Self-Determination and participatory governance across the data lifecycle (discussed further under legitimacy and trends).

Section III.

Principles, Legitimacy and Agency

11. How to develop data governance principles?

Developing data governance principles requires a structured, multi-step process. Various categories of principles guide different aspects of the data governance lifecycle, highlighting their interconnectedness and common overlaps. Key is to consider human rights frameworks as the foundation of any defining process. The process begins with defining clear objectives and the scope of governance to ensure alignment with the organization's strategy. Engaging stakeholders from diverse fields is crucial for inclusivity, relevance and trust. This engagement can be achieved through consultations, policy reviews, and benchmarking, which help to refine these principles. The principles should be categorized into governance processes, decision-making, and data handling. They must also be grounded in internationally recognized frameworks, such as human rights, data provenance, interoperability standards, and ethical AI guidelines, to ensure transparency, fairness, and adaptability. Finally, these principles should be embedded into governance structures and integrated into policies and workflows. It is essential to continuously review them to maintain their relevance in the ever-evolving legal and technological landscape.

12. What are the pillars of data governance?

The pillars of data governance encompass key principles that guide processes, decision-making, and data handling. Governance processes should be transparent, accountable, people-centered, fair, participatory, and lawful. Decision-making must be guided by transparency, proportionality, defined purpose, accountability, fairness, participation, and protection from harm and discrimination. Data handling requires confidentiality, security, proportionality, accessibility, privacy protection, informed consent, data quality, and interoperability. These pillars are further reinforced by global frameworks such as FIPPS, FAIR, FARR, CARE, and the OECD data-sharing principles.

13. How do cultural context and societal values shape data governance—and how can frameworks align with them?

Cultural differences in data governance stem from varying legal traditions, societal norms, and global frameworks. Principles such as transparency, accountability, lawfulness, fairness, and participation guide governance processes, yet their interpretation and implementation differ across regions. These differences shape data governance policies, influencing data provenance, interoperability, data access and re-use, privacy protection, and ethical considerations.

Organizations align their data governance frameworks with societal values by incorporating principles like transparency, accountability, fairness, and participation into their policies. They engage diverse stakeholders, including civil society and industry experts, to reflect ethical and cultural considerations. Regular policy reviews and benchmarking against frameworks like human rights or AI governance guidelines help organizations stay compliant and socially responsible. Scenario-based testing assessments also help measure the impact of governance policies, allowing adaptability to changing landscapes.

14. Through what processes should data governance principles be established?

Data governance principles should be established through a structured and iterative process that ensures alignment with legal frameworks, ethical standards, and societal values. The process begins with stakeholder engagement, where diverse voices—including government agencies, private sector actors, civil society, and technical experts—contribute to defining key principles. Policy review and benchmarking against existing legal and ethical frameworks, such as human rights conventions, data provenance and interoperability standards, and data ethics guidelines, help ensure consistency with global best practices. Organizations should also conduct workshops and consultation sessions to facilitate collaboration and refine governance principles. Additionally, scenario-based testing should be used to evaluate how these principles apply in real-world governance situations, ensuring they are practical, adaptable, and resilient to emerging challenges.

Tools like social license assessments and civic chartering can be used to gauge public acceptability and co-create normative frameworks through citizen juries, focus groups, and co-drafting exercises, surfacing localized priorities such as dignity, consent, and fairness.

15. How does the role of Indigenous data sovereignty fit within broader governance frameworks?

Indigenous data sovereignty asserts the right of Indigenous communities to govern the collection, use, and stewardship of their data in accordance with their laws, customs, and knowledge systems. It challenges state-centered and market-driven models by advocating for self-determination, ethical data practices, and culturally appropriate governance structures.

While broader governance frameworks prioritize data access, interoperability, and innovation, Indigenous data sovereignty emphasizes collective governance, benefit-sharing, and consent-based data practices. Recognized through frameworks like the CARE Principles, it is shaping global discussions on inclusive and ethical data governance by ensuring Indigenous participation in decision-making and respecting Indigenous worldviews on data stewardship.

16. What is social licensing and why is it relevant for data governance?

Social licensing refers to the practical and ongoing legitimacy that a data initiative earns from affected communities and the public—beyond formal legal permission. It is typically established through transparent engagement, participatory design, and accountability mechanisms that enable communities to articulate the values that should govern data use. Social license assessments and civic chartering are concrete methods for measuring acceptability and co-creating governance norms.

Social licensing is also directly connected to agency-based governance models such as Digital Self-Determination, which frames participatory decision-making 'based on a social license' as a way to move beyond one-time consent and toward continuous, adaptive control across the lifecycle.

17. How does data governance relate to 'technological determinism'?

A recurring governance risk in datafication is *technological determinism by default*: technical design choices (architectures, standards, interfaces, model constraints, logging defaults, access-control patterns) end up functionally determining what can be seen, proven, audited, contested, or enforced—so the system's design becomes the de facto governance regime. In practice, this means that 'what is governable' is shaped upstream by technical and organizational choices, not only by legal or policy intent. A data-governance framework counters this by treating technical design as a governance object: it requires technical literacy in decision-making; mandates documentation and provenance; builds auditability and traceability into systems; and ensures that accountability and remedies are operationally feasible (not merely declared). The goal is to prevent outcomes from being 'locked in' by opaque or path-dependent technical choices and to keep governance authority with accountable institutions rather than with system design and vendor defaults.

Section IV.

People, Institutions, Participation and Accountability

18. How can stakeholders be engaged to co-create effective data governance frameworks?

Stakeholders can be engaged through collaborative processes that ensure inclusivity, transparency, and alignment with legal and ethical standards. By fostering ongoing dialogue and feedback mechanisms, organizations can develop governance structures that are both effective and adaptable to evolving societal and technological needs. Workshops and consultation sessions allow diverse voices—including government agencies, private sector actors, civil society, and technical experts—to contribute to defining governance principles. Stakeholder mapping helps identify key actors and clarify their roles in data governance, ensuring a shared understanding of responsibilities. Policy review and benchmarking against global frameworks such as human rights conventions, data provenance standards, and ethical AI guidelines provide a foundation for informed decision-making. Scenario-based testing further refines governance frameworks by simulating real-world applications to identify gaps and ensure resilience.

19. How do we build capacity in data governance?

Building capacity in data governance requires a combination of training, stakeholder engagement, and structured frameworks to ensure effective data management throughout its lifecycle. Continuous education and technical training for data stewards, policymakers, and analysts help develop expertise in compliance, security, and ethical data use. Establishing clear governance structures, such as decision provenance models like RACI and data stewardship roles, ensures accountability and coordination. Stakeholder engagement through workshops, knowledge-sharing initiatives, and feedback loops fosters a culture of transparency and collaboration. Data management frameworks such as DAMA-DMBOK, maturity assessments, and audit tools help organizations evaluate and refine their governance practices. Investing in interoperability standards and metadata management further strengthens capacity by ensuring consistent, high-quality data handling across systems and sectors.

20. What are the most effective methods to enforce data governance policies? What tools and technologies support data governance implementation?

Enforcement requires (i) accountability structures with clearly assigned roles and responsibilities, (ii) monitoring and auditability across the lifecycle, and (iii) meaningful redress and remedies when harms occur.

Common enforcement methods include:

- Institutional oversight and escalation pathways (internal audit, compliance functions, independent review bodies).
- Transparency obligations (documented decisions, published standards where appropriate).
- Grievance mechanisms and accessible redress channels (administrative, judicial, ombudsperson pathways), with enforceable reparations where rights are violated.
- Periodic self-assessment and maturity reviews to identify gaps and prioritize improvements (used as a learning and prioritization tool, not only compliance).
- Tools and technologies that support implementation include contractual and procedural mechanisms (data sharing agreements, MOUs, SLAs), institutional policies and guidelines, and 'governance by design' approaches such as encryption, access controls, federated learning, differential privacy, audit trails, and interoperable metadata standards.

A practical enforcement caveat is technical complexity: when governance does not engage with technical nuance, enforcement can fail in practice (e.g., inability to evidence causal links, provenance, or lifecycle controls), effectively allowing system design to determine what is enforceable.

Section V.

Lifecycle Practices, Sectoral Regimes, Cross-Border Flows and Measurement

21. What are key characteristics of a Data Governance Framework?

Based on the above definition, the following characteristics will determine an effective and responsible data governance framework:

- **Human Rights-based approach:** Data governance must be firmly grounded in human rights. This includes safeguarding privacy, advancing self-determination, protecting freedom of expression, promoting non-discrimination, and ensuring the right to access information. As data plays an increasingly central role in shaping public and private life, governance frameworks must be designed to prevent harm, promote equity, and uphold the dignity and agency of individuals and communities.
- **Capacity Building:** Data governance is a highly specialized and constantly evolving field of practice. Policymakers, regulators, and practitioners need ongoing support to navigate the landscape. This requires that various forms of capacity building—including technical, legal and financial—be placed at the heart of any national or international approach to data governance.
- **Subsidiarity:** This characteristic emphasizes that decisions should be made at the most immediate or local level capable of addressing an issue. Given the deep impact of data on people's everyday lives, it is critical that the perspectives and priorities of communities at the grassroots level are reflected in the decision-making process. Toward that end localized capacity building is essential to ensure that data governance approaches are tailored to the specific needs, contexts, and realities of different communities.
- **Proportionality:** A foundational characteristic of effective data governance is proportionality—the principle that governance measures should be commensurate with the risks, sensitivity, and intended use of the data involved. Not all data or uses warrant the same level of control or scrutiny. Proportional governance ensures that safeguards, access controls, and decision-making processes are neither excessive nor insufficient, but instead tailored to the specific context, purpose, and potential impact of data use. This approach promotes efficiency, avoids unnecessary burdens on innovation or operations, and enhances trust by aligning governance intensity with actual societal, ethical, or legal stakes. Proportionality is especially critical in balancing competing imperatives such as openness and privacy, or innovation and protection, and should be reassessed regularly as data ecosystems evolve.

- **Resilience and Sustainability:** A data governance framework is effective only if it is consistent and predictable across time and contexts. For example, principles and incentives that wax and wane with changes in political or organizational leadership are unlikely to inspire trust and will lead to a weaker data ecosystem. It is therefore essential to build resilient and sustainable data governance institutions and systems that continue to function effectively despite changes in leadership, technological advancements, or external shocks.
- **Embedded and Inter-Sectoral:** Data governance is critical across many different sectors, ranging from healthcare, education, communications platforms, finance, transportation, environmental management, to national security. Each sector must manage its data assets while ensuring compatibility and coherence across governance systems. In addition, data is deeply intertwined with broader social, cultural, and political processes—it shapes how individuals are represented, how resources are allocated, how decisions are made, and how power is exercised. As such, data governance cannot be treated as a purely technical or administrative exercise; it must be embedded within wider human systems, reflecting societal values, addressing historical and structural inequalities, and fostering inclusive participation in the rules that govern data's use and impact.
- **Collaboration:** Today, the data ecosystem remains fragmented and siloed, with a persistent gap between the private control of data and its potential to serve the public good. Often, those best positioned to generate social value from data—such as researchers, public institutions, and civil society—face the greatest barriers to accessing it. Addressing this imbalance requires collaboration across sectors and disciplines, bridging public, private, academic, and civil society actors. Initiatives like data collaboratives and other partnership models have emerged as effective mechanisms to unlock data for the public interest—enabling more equitable access, fostering innovation, and supporting evidence-based policymaking.
- **Stewardship:** A central challenge in data governance is determining how to enable responsible access to data for use and reuse. Meeting this challenge requires the establishment of clear functions and the designation of individuals responsible for ensuring that data is accessed in a way that is systematic, sustainable, and aligned with public interest goals. This responsibility is best understood through the lens of stewardship rather than ownership. Within any data ecosystem, multiple stewards may exist—across companies, public sector bodies, and other institutions—each playing a role in managing data responsibly and facilitating its ethical and impactful use.

22. How do we move from principles to practices in data governance?

To implement data governance principles effectively, organizations must integrate them into structured processes, tools, and compliance frameworks across the data lifecycle. At the planning stage, defining roles, responsibilities, and legal requirements (e.g., GDPR, data protection acts) ensures alignment with broader regulatory frameworks. Data Management Frameworks (DAMA-DMBOK), Privacy Impact Assessments (PIAs), and Data Sharing Agreements (DSAs) help formalize compliance and collaboration.

Metadata and interoperability play a crucial role in operationalizing governance. New metadata and data provenance standards improve traceability, reliability, and decision transparency, ensuring that data remains usable and well-documented across its lifecycle. Interoperability frameworks, such as standardized data formats and data spaces, facilitate secure and efficient cross-organizational data exchange while maintaining compliance.

At the collection and processing stages, privacy-by-design frameworks, consent management tools, encryption, and audit trails ensure security and accountability. Decision provenance models (RACI) and governance scorecards track compliance and transparency, while regular stakeholder engagement, feedback loops, and maturity assessments help governance remain adaptable to evolving legal and technological landscapes.

23. How does data governance intersect with compliance requirements?

Data governance guides how data should be generated and (re)used, ensuring alignment with legal, regulatory, and industry-specific standards. It supports compliance with ethical guidelines, contractual obligations, and corporate policies, ensuring trustworthy, responsible and accountable data use across all contexts.

24. Is there a need for different data governance regimes for different sectors, such as healthcare or finance?

Yes, different sectors require tailored data governance regimes due to sector-specific risks, regulatory requirements, and data sensitivities. While core principles like transparency, accountability, and data quality remain universal, governance must adapt to each sector's legal, ethical, and operational needs. Since data governance is not one-size-fits-all, interoperability and metadata are vital to adapt governance frameworks to sector-specific needs, ensuring compliance, security, and efficiency while facilitating cross-organization and cross-border data flows.

25. Are there global standards for sector-specific data governance?

Some sector-specific data governance standards are truly global, while others are jurisdiction-based and apply at the regional or national level. Global standards are typically developed by international organizations and are widely adopted across various jurisdictions, ensuring interoperability and consistency. In contrast, jurisdiction-based regulations are enforced at the national or regional level. A global standard is generally a voluntary framework or a set of best practices that promotes consistency, interoperability, and ethical data governance across different jurisdictions. Examples of such standards include ISO 27799 (Health Informatics Security), FHIR (Healthcare Interoperability), ISO 21434 (Cybersecurity for Vehicles), and the OECD AI Principles. Organizations and governments can choose to adopt these guidelines; however, they become legally binding only when incorporated into national or regional legislation. Legally binding standards are usually jurisdiction-based and enforced by law. Examples include GDPR in the EU, HIPAA in the U.S., and PSD2 in financial services. Some global standards can also influence legal frameworks; for instance, Basel III for banking regulations has been widely implemented into national laws. Additionally, certain UN regulations, such as UNECE WP.29 for automotive cybersecurity, become mandatory for countries that are signatories. While global standards help shape governance policies, their legal enforceability depends on their adoption into regulatory frameworks at the national or regional level.

26. How should data governance address cross-border data flows?

Data governance must ensure that cross-border data flows comply with jurisdictional legislation, maintain security, and support interoperability. Different jurisdictions impose varying requirements; some favor data localization based on national security and policy concerns, while others promote shared trust, accountability, and harmonized frameworks. Requirements for local data storage can create inefficiencies and additional costs without clear benefits for privacy or local economies.

To address these challenges, organizations should engage with policymakers, regulators, and international frameworks to advance responsible data-sharing mechanisms. Governance structures should establish clear agreements on data transfers, ensuring compliance with sector-specific regulations while maintaining trust between entities. Mechanisms such as legal agreements, regulatory cooperation, and technological solutions, including privacy-enhancing technologies, can facilitate secure and efficient data exchange. Additionally, interoperability standards play a crucial role in reducing barriers to cross-border data flows while ensuring compliance with existing legal and governance frameworks.

27. How do organizations measure the success of their data governance initiatives?

Organizations measure the success of their data governance initiatives by assessing compliance, data quality, security, and overall governance maturity. Maturity Assessors evaluate data management capabilities against established governance models, ensuring that policies and practices align with regulatory and organizational standards. Regular compliance reviews conducted by the Compliance Team and Data Protection Officers (DPOs) help monitor adherence to legal frameworks such as GDPR. The effectiveness of Data Stewards is measured by improvements in data quality, responsible data access, and secure data sharing. Additionally, decision-provenance tools such as the RACI Model ensure clear accountability and traceability in governance decisions, enhancing transparency and operational efficiency. Continuous assessment and refinement of governance practices help organizations maintain alignment with evolving legal, ethical, and technological landscapes.

28. How can data governance support the safe use of AI?

Data governance supports the safe use of AI by ensuring that training and operational data is high-quality, representative, and well-documented (including provenance/metadata), handled lawfully with appropriate access controls, privacy and security safeguards, and risk/impact assessments, and governed through auditability and accountability mechanisms across the lifecycle. These controls operationalize the 'trustworthy, human-rights-respecting' expectations reflected in the OECD AI Principles and in G7 instruments such as the G7 Toolkit for AI in the Public Sector and the Hiroshima AI Process (including its Reporting Framework), which emphasize transparency, oversight, and accountability—capabilities that depend on robust data governance.

Section VI.

Cross-Cutting Considerations and Future Directions

29. What are cross-cutting considerations for data governance?

- **Acknowledging Diversity:** Countries are at different stages of developing data governance policies. Some have advanced systems, while others are just beginning to establish the necessary legal and technical foundations. While many countries have developed robust frameworks for personal privacy and data protection, fewer have made comparable progress in enabling responsible access to data for use and reuse—a gap that increasingly limits the potential for innovation and public benefit. In addition, countries vary widely in their technical, legal, and financial capacities. As a result, one-size-fits-all solutions are insufficient; any governance framework must be adaptable and responsive to these diverse contexts and capabilities.
- **Learning from Practices:** A wide and growing body of evidence and learnings now exists on data governance—what works, and what doesn't—from around the world. Countries with mature governance systems can offer valuable lessons (including mistakes made) to those just starting; policymakers can also adapt findings from jurisdictions with similar cultural, social, or political contexts. Any national-level data governance framework should therefore be built on the foundation of case studies and sharing of human rights-based practices derived from other regions.
- **Focus on Inclusivity:** Inclusive data governance ensures that all stakeholders—notably those from underrepresented groups—can participate in shaping policies and benefit from data use (and re-use). This includes the ability to help determine what data is collected, how it is used, and under what conditions. Respect for consent and attention to differing needs and sensitivities are key to building fair and effective systems.
- **Balancing Data as a Public Good vs. Private Right vs. Commercial Asset:** Effective data governance must strike a careful balance between multiple roles that data can play. While some data may be treated as a public good—freely available and non-rivalrous—other datasets may be restricted for legitimate reasons, such as privacy, national security, or commercial confidentiality, yet still serve critical public interest purposes. Conversely, not all openly available data necessarily benefits the public interest. Governance frameworks must therefore distinguish between openness for openness's sake and responsible, purposeful data use that advances societal well-being. This includes enabling the reuse of data for innovation and service delivery, particularly in areas like AI and health, while ensuring strong protections against misuse, discrimination, and rights violations. Balancing these interests is one of the most sensitive but essential challenges of modern data governance—central to realizing data's full societal potential without undermining individual or collective rights.

30. What are some trends in data governance?

Data governance is a dynamic process. Policymakers must constantly contend with the accelerating pace of technological innovation, which often outstrips regulatory systems' ability to keep up. Data governance, therefore, must be agile, responsive, and future-facing—capable not only of addressing current challenges but also of anticipating those on the horizon. While governments have traditionally borne the burden of foresight, a growing trend in modern digital regulation is to place foresight and risk-management duties on technology developers and platform operators themselves—requiring measures such as risk/impact assessments, transparency and documentation, testing and monitoring, and meaningful stakeholder engagement. In doing so, these approaches acknowledge that those who profit from data-driven systems must also be accountable for anticipating and mitigating potential harms. Foresight, in this sense, is no longer solely a public responsibility—it is becoming a shared duty across the data ecosystem.

Some ongoing trends in data governance, which may affect the way data policies are designed and implemented, are:

- **From Misuse to Missed-Use:** Historically, data governance has predominantly been focused on data protection and ensuring compliance with privacy and security regulations. Such policies were designed to prevent individual harm and misuse. Over time, the need for more focus on the risks of missed use have become apparent. In particular, as the benefits of repurposing private data for public good have become apparent, there is growing recognition that policy must extend and complement governance frameworks to permit legitimate, justified forms of data access, sharing, and reuse. This is part of a broader recognition of data as a valuable social and development (not just commercial) asset that requires not just protection but stewardship (see above)—balancing the need to safeguard data with the imperative to make it accessible for innovation, public good, and sustainable development.
- **Balancing Innovation with Compliance:** As the demand for robust data governance grows, so too does the recognition that regulation and innovation are not opposing forces—they can and should reinforce one another. Well-designed governance frameworks can enable more responsible, resilient, and socially beneficial forms of innovation. Tools such as data sandboxes illustrate this principle in practice: they create controlled environments where organizations can test data-driven solutions while managing risks, complying with regulatory requirements, and engaging relevant stakeholders. Similarly, the use of synthetic data is gaining momentum as a privacy-preserving method that supports experimentation, particularly in sensitive domains like health and AI development. Emerging architectures such as data mesh

and federated systems are also redefining traditional centralized models of data control, promoting decentralized, context-aware, and collaborative data stewardship. Together, these approaches show how innovative practices can be aligned with—and even enhanced by—strong governance principles, ensuring that experimentation does not come at the expense of ethics, equity, or environmental sustainability.

- **Equity and Inclusiveness:** The often siloed, centralized nature of the data ecosystem has raised growing concerns about equity and inclusiveness in the data economy. In particular, the global trade in data has been criticized for reinforcing existing patterns of social and economic marginalization, both within and between countries. As a response, policymakers are increasingly called upon to design new, more equitable approaches to data governance—ones that account for historical asymmetries, power imbalances, and systemic bias. Concepts such as data colonialism highlight how current data flows and ownership models can reproduce global extractive dynamics, disproportionately benefiting actors in the Global North while limiting agency and value creation in the Global South. Similarly, data feminism draws attention to how gender, race, and other structural inequalities shape the way data is collected, categorized, and used. These perspectives have converged in a growing movement for data justice, which seeks to ensure that data systems not only avoid harm but also actively contribute to fairness, representation, and empowerment. To translate these critiques into action, data governance frameworks must move beyond neutrality and incorporate equity-by-design principles. This includes embedding participatory governance mechanisms, representational safeguards, and benefit-sharing models into data policy and infrastructure. It also requires supporting localized governance structures, recognizing community data rights, and ensuring that marginalized voices are not only protected but also empowered in the stewardship and reuse of data. In doing so, data governance can become a tool not just for managing data, but for actively redressing imbalances and fostering justice in the digital age.
- **Digital Self-Determination (DSD):** In part in response to concerns about inclusiveness, an emerging approach to data governance emphasizes empowering individuals and communities to maintain ongoing control over their data throughout its lifecycle. This approach differentiates itself from static consent models by seeking to ensure dynamic, participatory involvement in decision-making about datafication, data collection, ownership, processing, sharing, and deletion. Digital Self-Determination can be articulated as a data governance principle that seeks to preserve and strengthen meaningful individual and community agency over decisions across the data lifecycle—so that participation, accountability, and contestability are operational rather than merely formal. While UN-system documents do not consistently use the

term Digital Self-Determination as a named principle, international data-governance work increasingly frames equity as including agency, and emphasizes empowering data subjects and communities to influence how data is collected, used, shared, and governed (e.g. UN System CEB/2024/2/Add.1). This principle is developed and operationalized in Verhulst (2023).

- **Generative AI and AI-Ready Data:** The rise of generative AI presents both new challenges and opportunities for data governance. For instance, as AI systems become more capable of creating their own data, making predictions, and generating new insights from vast datasets, data governance frameworks need to evolve to address these shifts. Generative AI also introduces new complexities related to data sourcing, model transparency, ethical use, and regulatory compliance that traditional data governance models may not fully accommodate. For example, data provenance and quality are emerging as critical issues to avoid perpetuating biases or producing harmful outputs. In addition, data governance must address issues such as copyright, liability, and accountability for AI-generated content (e.g., misinformation or incorrect advice). All these issues—and many more—are likely to dominate the data governance landscape over the coming years, making it essential for policymakers to remain up to speed and aware of emerging AI trends.

Additional Guidance on Data Governance

Toolkit	Audience
Data Governance Toolkit: Navigating data in the digital age (UN Broadband Commission)	Public Sector
Data Governance Toolkit (NSW Government Agencies)	Public Sector
Data Governance Framework (Australian Government)	Public Sector
The Data PlayBook (IFRC and Solferimo Academy)	Humanitarian Sector
Data Responsibility Journey (The GovLab)	Public and Private Sector
Data Innovation Toolkit (European Commission Digital Innovation Lab)	Public Sector
Navigating Data Governance (ITU)	Regulators
Data Governance and Management Toolkit (SGIG DSC Members)	Self-Governing Indigenous Governments
Data Governance Workbook (Digital Civil Society Lab)	Non-Profit Sector
Data Governance Toolkit (Nethope)	Non-Profit Sector
OECD Data Governance page	Public Sector
Data to Policy Navigator (UNDP)	Public Sector
Data Governance Knowledge Sharing (Albireo Group)	Non-Profit Sector

References

Albireo Group. *Data Governance Knowledge Sharing*. Accessed February 9, 2026. https://www.albireogroup.com/data-governance-knowledge-sharing.

Australian Government, Department of Finance. *Data Governance Framework*. Canberra: Australian Government, September 2025. https://www.finance.gov.au/sites/default/files/2025-09/Data-Governance-Framework.pdf.

Broadband Commission for Sustainable Development Working Group on Data Governance. *Data Governance Toolkit: Navigating Data in the Digital Age*. By Stefaan G. Verhulst, with contributions by Leona Verdadero. Geneva: Broadband Commission for Sustainable Development, July 2025. https://www.broadbandcommission.org/wp-content/uploads/2025/07/Data-Governance-Toolkit.pdf.

Calac, Alec J., and Timothy K. Mackey. "Indigenous Data Sovereignty for Indigenous Peoples in the Era of Big Data." *npj Digital Medicine* 8 (2025): 504. https://doi.org/10.1038/s41746-025-01902-w.

Carroll, Stephanie R., Ibrahim Garba, Oscar L. Figueroa-Rodríguez, Jarita Holbrook, Raymond Lovett, Simeon Materechera, Mark Parsons, Kaitlin Raseroka, Desi Rodriguez-Lonebear, and Robyn Rowe. "The CARE Principles for Indigenous Data Governance." *Data Science Journal* 19, no. 1 (2020): 43. https://doi.org/10.5334/dsj-2020-043.

European Commission. "Digital Innovation Lab (iLab)." *Interoperable Europe Portal*. Accessed February 9, 2026. https://interoperable-europe.ec.europa.eu/collection/european-commission-digital-innovation-framework/solution/digital-innovation-lab-ilab.

International Federation of Red Cross and Red Crescent Societies (IFRC) and Solferino Academy. *Data Playbook Toolkit v1*. June 21, 2022. https://preparecenter.org/toolkit/data-playbook-toolkit-v1/.

International Telecommunication Union (ITU) and World Bank. *Navigating Data Governance: A Guiding Tool for Regulators*. Digital Regulation Platform. Updated June 11, 2025. Accessed February 9, 2026. https://digitalregulation.org/toolkit/navigating-data-governance/.

NetHope. *Data Governance Toolkit: A Guide to Implementing Data Governance in Nonprofits*. Accessed February 9, 2026. https://nethope.org/toolkits/data-governance-toolkit-a-guide-to-implementing-data-governance-in-nonprofits/.

NSW Government, Data Analytics Centre (Data.NSW), Department of Customer Service. *NSW Data Governance Toolkit*. Version 1.1. February 2021. https://data.nsw.gov.au/sites/default/files/inline-files/NSW%20Data%20Governance%20Toolkit%20V1.1.pdf.

OECD and UNESCO. *Toolkit for Artificial Intelligence in the Public Sector*. Paris: OECD Publishing, 2024. https://doi.org/10.1787/421c1244-en.

OECD. *Recommendation of the Council on Artificial Intelligence*. OECD/LEGAL/0449. Paris: OECD, May 2019 (as amended). https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

OECD.AI. "Hiroshima AI Process." Accessed February 9, 2026. https://oecd.ai/en/hiroshima-ai-process.

Reutter, Lisa, and Heidrun Åm. 2024. "Constructing the Data Economy: Tracing Expectations of Value Creation in Policy Documents." *Critical Policy Studies* 18 (4): 639–59. https://doi.org/10.1080/19460171.2023.2300436.

Self-Governing Indigenous Governments (SGIG) Data Project. "Indigenous Data Toolkit (Data Governance and Management Toolkit for Self-Governing Indigenous Governments)." Accessed February 9, 2026. https://indigenousdatatoolkit.ca/.

Solferino Academy. "Your Data Playbook Is Ready. Download It Now!" June 21, 2022. Accessed February 9, 2026. https://solferinoacademy.com/your-data-playbook-is-ready-download-it-now/.

United Nations Conference on Trade and Development (UNCTAD). "26th CSTD Side Event: From Data Protection to Data Empowerment: Good Practices from around the World on Data Spaces, Data Commons and Data Governance." March 28, 2023. Accessed February 9, 2026. https://unctad.org/meeting/26th-cstd-side-event-data-protection-data-empowerment-good-practices-around-world-data.

United Nations System Chief Executives Board for Coordination, High-Level Committee on Programmes. *International Data Governance: Pathways to Progress*. New York: United Nations, May 2023. https://unsceb.org/international-data-governance-pathways-progress

United Nations System Chief Executives Board for Coordination, High-Level Committee on Programmes. *Proposed Normative Foundations for International Data Governance*. CEB/2024/2/Add.1. New York: United Nations, 2024. https://unsceb.org/sites/default/files/2024-11/CEB_2024_2_Add.1_Normative%20Foundations%20for%20International%20Data%20Governance%20%28final%20advance%20unedited%29.pdf.

Verhulst, Stefaan G. "Operationalizing Digital Self-Determination." *Data & Policy* 5 (2023): e44. https://doi.org/10.1017/dap.2023.11.

Verhulst, Stefaan G., Adam Zable, Andrew Zahuranec, and Peter Addo. "Reimagining Data Governance for AI: Operationalizing a Social License for Data Reuse." SSRN Scholarly Paper no. 5255677. New York: The GovLab, 2025. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5255677.

OECD. "Data Governance." *OECD*. Accessed February 9, 2026. https://www.oecd.org/en/topics/sub-issues/data-governance.html.

The GovLab. *Data Responsibility Journey*. Accessed February 9, 2026. https://dataresponsibilityjourney.org/.

United Nations Development Programme (UNDP). *Data to Policy Navigator*. Accessed February 9, 2026. https://datatopolicy.org/.

Stanford PACS Center on Philanthropy and Civil Society. *Data Governance Workbook*. data.org. Accessed February 9, 2026. https://data.org/resources/data-governance-workbook/.

GOVLAB

WHAT IS DATA GOVERNANCE: 30 QUESTIONS AND ANSWERS

A practical reference for policy, institutional, and operational design