

**INTERSESSIONAL PANEL OF THE UNITED NATIONS COMMISSION ON
SCIENCE AND TECHNOLOGY FOR DEVELOPMENT (CSTD)**

**Geneva, Switzerland
6 November 2026**

Contribution by Brazil

**to the CSTD 2026-2027 priority theme on
“Data Governance for Development: From Asymmetry to Equitable Stewardship”**

DISCLAIMER: The views presented here are the contributors' and do not necessarily reflect the views and position of the United Nations or the UN Trade and Development.
--

Table of Contents

Various federal government agencies were consulted. Below are the responses to the questionnaire, with contributions from Brazil's Ministry of Science, Technology and Innovation (MCTI); Ministry of Development, Industry, Trade and Services (MDIC); Ministry of Justice and Public Security (MJSP) Information and Communication Technology Sub-Secretariat; Data Governance and Management Coordination-General and National Secretariat for Digital Rights: Data Protection Coordination-General; National Data Protection Authority (ANPD); Data Processing and Information Technology Company for Social Security (Dataprev) and Ministry of Health (MS)

1) Can you share challenges that your country face in building and leveraging data capacities, including issues related to infrastructure, ownership and stewardship, free and trusted cross-border flows, and benefit-sharing? (Please provide examples and, where possible, quantitative evidence or indicators of these challenges and their impacts)

Ministry of Science, Technology and Innovation (MCTI)

Brazil continues to face a structural deficit in hardware infrastructure, particularly with regard to semiconductors and computing accelerators, as well as a significant dependence on foreign cloud service providers (hyperscalers), which may give rise to risks of vendor lock-in and geopolitical vulnerabilities. In addition, challenges persist with respect to meaningful connectivity, the underinvestment in critical infrastructure, and the further development of the regulatory framework, all of which constrain the effective governance of the country's digital assets. These challenges have been documented in recent studies, particularly "Soberania Digital no Brasil: diagnóstico, desafios e caminhos sob a perspectiva da ciência, tecnologia e inovação," prepared under the Digital Technologies Observatory, an initiative of the Ministry of Science, Technology and Innovation (MCTI) and the Center for Management and Strategic Studies (CGEE). These vulnerabilities are being addressed through the implementation of public policies, most notably the Brazilian Artificial Intelligence Plan (PBIA). The Plan seeks to address infrastructure gaps and technological dependence through a range of strategic initiatives, including the acquisition of a high-performance supercomputer, the establishment of a Sovereign Cloud, and the leveraging of Brazil's clean energy matrix to foster a sustainable and environmentally responsible artificial intelligence infrastructure.

Ministry of Development, Industry, Trade and Services (MDIC)

In the context of the productive sector, data lies at the center of the economy's digital transformation process, as it is fundamental to the development of advanced digital technologies such as artificial intelligence (AI), big data analytics, machine learning, and cloud computing, among others. This new scenario presents significant potential for the strategic use of data by productive sectors, but this potential is currently limited by structural and institutional obstacles, among which the following stand out: (i) low digitalization and technological heterogeneity across production chains; (ii) difficulty in accessing data generated by embedded devices and the concentration of data ownership/control in service platforms; (iii) legal and technical uncertainty regarding data sharing between companies, given the absence of a legal framework for non-personal and industrial data; (iv)

lack of knowledge, literacy, and data management capabilities as a strategic asset among companies; and (v) the absence of clear guidelines for sharing government data with the productive sector.

Brazil demonstrates a high aptitude for adopting data-based services, considering that 85% of the population has internet access and the country shows broad adoption of digital platforms — such as GOV.BR, which exceeds 175 million users — as well as high readiness for data reuse, evidenced by the availability of more than 19,000 open databases. However, a gap remains in stimulating the use and sharing of data. Evidence of this is information from ABINC indicating that 86% of industrial data is not used and remains “siloed” due to a set of legal, technical, and cultural barriers.

To understand the maturity of the Brazilian context on this issue, a call for input was conducted between March and April 2026 by the Brazilian Agency for Industrial Development (ABDI), in partnership with MDIC, which produced relevant evidence regarding the needs identified by respondents to enable the use and sharing of data by their organizations:

Regulatory Framework: 81% highlight the need for legal certainty for data use and sharing.

Governance: approximately 57% point to the need for ongoing audit and compliance for data use and sharing, and indicate the importance of defined technical standards.

Fostering and Technological Solutions: approximately 50% indicate the need for secure and reliable infrastructure and highlight the importance of pilot environments for testing and experimentation.

Awareness, Training, and Capacity-Building: 44% point to the need for staff training and skills to work with data.

Other relevant data collected show that 55% of respondents already provide or access data from other organizations, 67% are interested in obtaining market data, and 66% responded that the most valuable data types from partners in their supply chain are “Supplier Data.”

The survey results not only highlight the main existing barriers but also guide pathways for the implementation of public policies.

Ministry of Justice and Public Security (MJSP) — Information and Communication Technology Sub-Secretariat

The challenges include the need to establish a set of strategic guidelines to be agreed upon among public organizations of the three branches of government — executive, legislative and judiciary — with clear programs for implementing data governance and management policies aimed at strengthening the processes, tools, and monitoring of results to be rolled out in each public body, especially those of the executive branch.

With regard to data governance policies, there is a need to govern the harmonization of institutional structures and arrangements for the provision of specialized information and communication technology (ICT) services and capacities for data processing, considering solutions that ensure pre-qualification of service providers — whether companies or specialized professionals — and/or pre-arranged relationships with major market players providing solutions, as well noted in the ANPD’s submission (SEI No. 36256681), when addressing the issue of data ownership and management, namely:

“The lack, within national territory, of adequate technological infrastructure to process high volumes of data has generated strong dependence on foreign solutions, especially those provided by so-called Big Techs. According to a survey conducted by GETIP/USP and GEPSI Data/UnB, the Brazilian public sector contracted, between 2014 and 2025, at least R\$23 billion in information and communication technology (ICT), with the largest contracts signed with only 4 companies — Microsoft, Oracle, Google and Red Hat. In addition, it is estimated that dependence on foreign digital services generated a deficit of US\$6.8 billion in the Brazilian trade balance in 2024.” (p.2, 36256681)

It is also necessary to promote the harmonization of functional structures, career paths, technical staff of civil servants and contracted collaborators, as well as investments in the design of ICT and data units with effective capacity to respond broadly to the challenges of public policies supported by the Executive Branch, thereby ensuring better management of demands, use and reuse of data with broad legal support and practical, effective attention to the Brazilian legal framework, especially the LGPD (General Data Protection Law).

Formalize and develop, through academic and technical training, the role of Data Curators, to be filled by permanent federal civil servants who can draw on a network of specialized and innovation-related expertise in order to act with full awareness of the value of data assets and their social impacts when serving public policies and/or as drivers of public policies benefiting citizens.

When referring to the harmonization of structures and institutional arrangements for the provision of ICT services and capacities, we highlight already successful initiatives such as the “Acelera MJ” program, which provided secure, fast, and autonomous access for MJSP managers to develop their software solutions using Low Code technology.

However, this initiative itself, among others such as the provision of SSBI (Self-Service Business Intelligence), needs to develop based on the aforementioned fundamentals and still requires harmonization of organizational structures to avoid so-called Shadow IT, which ends up “isolating” data assets from corporate and institutional oversight and treatment, contributing to the formation of “silos” and hindering the convergent and shared use of data, information, and knowledge in service of society, particularly regarding Justice and Public Security issues.

Ministry of Justice and Public Security (MJSP) — National Secretariat for Digital Rights, Data Protection Coordination-General

Brazil holds a prominent position in the global digital ecosystem: it is the world’s fifth-largest internet market and the largest in Latin America in number of users. As in much of the developing world, a significant portion of the data generated by the population is processed and stored by global platforms. The country has actively sought to develop strategies to strengthen its data infrastructure and promote governance that favors national development.

The General Data Protection Law (LGPD) and the work of the National Data Protection Authority (ANPD) introduced modern regulatory mechanisms that allow the Brazilian State to ensure the protection of its citizens’ personal data, in line with international best practices. The country remains committed to improving mechanisms for international cooperation to optimize the application of these rules in a globalized digital environment.

CD/ANPD Resolution No. 19/2024 established the Regulation on International Transfer of Personal Data, setting solid legal bases for transfers, such as standard contractual clauses and binding corporate rules. Brazil has maintained constructive dialogues with international partners, including the European Union, aiming to facilitate bilateral data flows, which will contribute to the competitiveness of Brazilian companies in the global market.

The ANPD’s Guidance Document on International Transfer (2023) provides valuable practical guidance for the market. The Brazilian government continues working to expand bilateral and multilateral agreements, seeking to offer an increasingly predictable and secure business environment for companies of all sizes, with special attention to micro and small enterprises and startups.

Regarding benefit-sharing, Brazil has fostered debates on economic models that promote a more balanced return of the value generated by data to Brazilian society, encouraging local innovation and the development of national technological solutions.

The National Data Protection Authority, created in 2020 and elevated to regulatory agency status in 2026, began its activities with a reduced structure and has gradually expanded its technical and sanctioning capacity. The 2023 Management Report of the National Data Protection Authority records significant growth in the number

of complaints received (more than 3,000 in 2023), which demonstrates growing citizen awareness of data protection rights, but also reveals the growing demand for a more robust institutional structure.

The 2023 ICT Households survey conducted by CGI.br indicates that, although internet penetration in Brazil reached 84% of households, significant regional asymmetries persist: in the North and Northeast regions, access is below the national average, which impacts the ability of citizens in those regions to effectively exercise their digital rights. This data, although falling under the Ministry of Communications' connectivity policy competence, has direct implications for the effectiveness of the data protection framework.

Decree No. 10,046/2019 regulated data-sharing governance within the federal Executive Branch, establishing the Citizen's Base Registry and the Central Data Governance Committee (CCGD). The operationalization of these mechanisms has progressed, but the challenge remains of harmonizing personal data protection principles — especially minimization and purpose limitation — with the goals of administrative efficiency and interoperability of government databases.

Data Processing and Information Technology Company for Social Security (Dataprev)

The challenges faced by Brazil in building and leveraging data capacities are multidimensional in nature, encompassing technical, semantic, institutional, regulatory, and organizational aspects.

On the technical front, the heterogeneity of government information systems stands out, characterized by the coexistence of legacy solutions, diverse data models, and differing levels of digital maturity among public bodies. This scenario imposes limitations on interoperability, requiring the adoption of standardized interfaces, service-oriented architectures, and API-based integration mechanisms.

From a semantic perspective, there is a need to harmonize controlled vocabularies, taxonomies, and data models — an essential condition for ensuring consistency, interoperability, and information quality.

At the institutional level, challenges relate to inter-organizational coordination, the clear definition of roles and responsibilities, and the need for alignment among entities with differing technical and operational capacities.

From a regulatory standpoint, the main tension lies in reconciling data sharing with adherence to personal data protection principles, especially those established by the General Data Protection Law (LGPD), as well as in managing cross-border flows in an international scenario marked by regulatory fragmentation.

At the organizational level, there is a need to strengthen the data governance culture, adopt structured information quality management practices, and provide continuous training for human resources.

Associated risks include registration inconsistencies, duplicate records, difficulties in uniquely identifying individuals, the propagation of errors across interconnected systems, and undue exposure of sensitive data.

National Data Protection Authority (ANPD)

In a global context marked by intense informational flows and by countries and societies that are increasingly interconnected digitally, data has emerged as a strategic resource for development and innovation. However, inequalities in terms of data access, available infrastructure, and governance capacity generate new asymmetries while also reinforcing existing ones.

In this scenario, Brazil, as a developing economy, still faces a series of challenges in building and leveraging data capacities. Although it has advanced consistently in building data-related capacities — especially following the entry into force of the General Data Protection Law (LGPD — Law No. 13,709/2018) and the institutional strengthening of the National Data Protection Authority (ANPD) as a regulatory agency — structural and regulatory challenges persist that impact the full realization of these capacities, particularly with regard to infrastructure, ownership and stewardship, cross-border flows, and benefit-sharing.

Regarding infrastructure, the shortage of high-performance computing (HPC) systems, including graphic processing units (GPUs), stands out. These systems, which enable the processing of high volumes of data — as required for training and running artificial intelligence (AI) models — are housed in data centers, a fundamental pillar of data infrastructure. According to a NIC.br study, it is estimated that, between May and June 2025, Brazil had 465 private data centers and 89 public-sector data centers[1]. Although this survey used its own methodology, which makes it difficult to compare the resulting figure with quantities for other countries, Data Center Map data can be used for this purpose: according to that database, as of May 20, 2026, Brazil had 208 data centers[2], while Western Europe had 2,781[3] and the United States had 4,286[4]. In other words, compared to traditional centers of power, Brazil still has a very small number of data centers. Added to this is the diagnosis by the Ministry of Finance, according to which there persists a "high national dependence on digital services provided abroad, currently reaching around 60% of national digital workloads"[5].

Brazil's data infrastructure rests on broad mobile connectivity and growing internet penetration, but it continues to be marked by significant differences between regions and types of access[6]. Fixed home internet penetration remains lower than mobile penetration, reflecting a dependence on mobile networks for data generation and consumption[7]. Urban centers, especially in the Southeast, concentrate data centers, internet exchange points (IXPs), and greater availability of fiber optics, supported by submarine cables and international backbone infrastructure[8], while the North region and parts of the Northeast face limited coverage, higher latency, and fewer interconnection options. These asymmetries reduce local capacity to produce, store, and process data, in addition to increasing operational costs for regional actors. Connectivity inequalities directly impact digital inclusion, access to digital public services, and the development of the data economy, conditioning representative data collection and information sharing[9]. Access gaps in rural areas and urban peripheries hinder participation in digital platforms and constrain initiatives such as telemedicine, distance learning, and electronic public services — effects documented during the COVID-19 pandemic, when remote teaching and remote care revealed major disparities in reach and quality[10].

In this same context, another point requiring attention, and one that brings its own challenges, concerns the natural and energy resources needed to install and maintain data centers. According to a Brasscom study, in 2024, 1.7% of the electricity consumed in Brazil was directed to data centers, and this percentage is estimated to rise to 3.6% by 2029. Beyond electricity, there are also concerns about water consumption, given the need to cool these systems. The same study indicates that, in 2022, data centers accounted for 0.003% of consumptive water use in Brazil, corresponding to approximately 2 billion liters, with an increase to 0.008% projected for 2029[11].

Although Brazil's energy and geographic circumstances are, in general, quite favorable (with an energy matrix that is 89% renewable, ample land availability, and low risk of natural disasters), and data center systems tend to have increasingly greater water and energy efficiency, environmental concerns cannot be dismissed. In energy terms, demand concentrated in a single location generates risks to distribution stability and to tariff increases; in water terms, risks arise related to water supply in regions marked by scarcity or water stress[12]. Furthermore, as noted by Professor Fernando Caneppele (USP), there are challenges stemming from the lack of planned integration between renewable energy generation — such as solar and wind, which are intermittent — the concentration of energy availability in certain regions, and, additionally, the operation of the hydroelectric matrix near its limit in some scenarios[13].

Closely related to the challenges mentioned above is also the issue of data ownership and management. The lack, within national territory, of adequate technological infrastructure to process high volumes of data has generated strong dependence on foreign solutions, especially those provided by so-called Big Techs. According to a survey conducted by GETIP/USP and GEPSI Data/UnB, the Brazilian public sector contracted, between 2014 and 2025, at least R\$23 billion in information and communication technology (ICT), with the largest contracts signed with only four companies — Microsoft, Oracle, Google, and Red Hat. In addition, it is estimated that dependence on foreign digital services generated a deficit of US\$6.8 billion in the Brazilian trade balance in 2024[14].

It should be noted that Brazil has a consolidated legal framework for data protection and governance in the LGPD and the ANPD, as the central body for implementation, oversight, and enforcement. These instruments are fundamental to the materialization of data stewardship, as they establish rules on the legal bases for processing, data subjects' rights, accountability, and international transfer mechanisms that underpin the attribution of duties and trust in the digital ecosystem. However, the effectiveness of this apparatus depends on robust institutional capacity, through the continuous allocation of technical and human resources to the ANPD, the enhancement of regulatory competencies, effective inter-institutional coordination, and regulatory clarity on emerging issues.

More than an economic burden, this scenario brings with it concerns of a political, legal, and social nature, insofar as Brazilian data ends up "under the tutelage" of other countries. In other words, storage on servers of foreign companies threatens Brazil's ownership and management of its own data, making it vulnerable to sanctions and surveillance laws of other nations.

Still within the scope of data management, another challenge that arises concerns interoperability, both within the Brazilian public sector itself and between the public and private sectors. Difficulties emerge especially in the health sector, in which systems used by clinics and/or private health plans are often incompatible with those used by the Unified Health System (SUS). Within SUS itself, there also persists an overlap of different digital systems and architectures. As an illustrative example, it is estimated that, since 1990, SUS has accumulated more than 400 distinct systems[15]. This fragmentation not only creates data silos but also hinders the adoption of national technical guidelines and standards. In practice, this has a direct impact on service delivery, at times generating rework, creating an additional layer of bureaucracy for citizens, and hindering the agile formulation of public policies. In the health field, this compartmentalization can directly affect patients, resulting, for example, in unnecessary repetition of tests and delays in providing an adequate diagnosis.

In addition, Brazil's capacity to effectively exercise ownership and management over its own data may also encounter barriers in unrestricted cross-border flows. In this context, the main challenge stems from the need to strike a balance between maintaining the necessary flows, so as to ensure the availability of information, and regulation that guarantees due protection of data, safeguarding data subjects' rights.

Through the LGPD, Brazil adopts a model that allows international transfers of personal data conditioned on adequate safeguards, such as contractual clauses, adequacy decisions, and binding corporate rules, as regulated by the ANPD through CD/ANPD Resolution No. 19, of August 23, 2024 (International Data Transfer Regulation). Earlier this year, in 2026, the adequacy decision between the European Union and Brazil was published, recognizing that both offer equivalent levels of data protection, thereby facilitating the international transfer of personal data between these territories. This decision simplifies data circulation and reduces operational costs and legal risks for organizations carrying out data flows between Brazil and the EU. Despite this, the country still has persistent challenges related to other territories, which require harmonization with different legal regimes — for example, the lack of equivalence between the LGPD and United States frameworks, which can generate regulatory complexity for multinational companies.

Additionally, the national legal order establishes principles and duties applicable to data processing operations, including in international transfer scenarios, insofar as the LGPD establishes legal bases, principles, and controller and operator obligations that apply regardless of where processing occurs. The ANPD has confirmed, in its guidance and regulations, that responsibilities for security and governance measures persist in cross-border transfers, and that adequacy instruments or contractual safeguards do not remove the obligation to effectively protect data subjects' rights. Nonetheless, the coexistence of diverse regimes imposes regulatory complexity on multinational companies, which must reconcile different legal requirements without prejudice to the protection duties set out in Brazilian legislation. It is worth noting that domestic data protection and information security measures constitute legitimate public regulatory practices and should not be automatically interpreted as undue barriers to digital trade; multilateral organizations and trade forums recognize the

compatibility between data protection policies and trade facilitation, provided that proportionate and transparent principles are observed[16].

The implications of this imperative are multifaceted: for the private sector, it means adjusting policies and processes — and, in some cases, organizational structures — to ensure compliance with current regulations. This adjustment, however, can entail high costs, especially for small and medium-sized enterprises. For the Brazilian State, and more specifically for the ANPD, it means developing and overseeing transfer and sharing mechanisms that enable the international flow of data while simultaneously ensuring that the destination country offers a level of protection equivalent to that of the LGPD. This regulatory and oversight role, however, requires timeliness in addressing emerging concerns and must take into account the interests of other political and economic actors. For example, it is important that mechanisms to regulate cross-border data flows do not hinder the full realization of economic activities and do not create obstacles in the diplomatic field.

Furthermore, at the global level, there is also the challenge of qualitatively equalizing cross-border data flows. This is because international data flows are still strongly characterized by a "South-North" dynamic, in which developing countries of the Global South send raw data to developed countries of the North, which, in turn, "refine" it and transform it into intelligence. In this scenario, developing countries, such as Brazil, run the risk of becoming mere suppliers of raw data to large digital platforms of the Global North, while at the same time being obliged to pay for the digital intelligence obtained from their own data[17].

Finally, these inequalities reverberate directly in the distribution of benefits that can be obtained, insofar as one of the most important parts of the data value chain — namely, its processing and transformation into intelligence — ends up concentrated in the hands of a small number of digital platforms. Added to this is the fact that the agents that control data, and the location from which that data is controlled, directly influence the advantages that can be obtained from it. Given this context, Brazil also faces the challenge of maximizing the benefits it obtains from its data, seeking to advance models that ensure that the economic and social value of data is shared in a more inclusive manner.

This challenge, however, is far from being restricted to the international scenario; it also applies to the country's internal reality, marked by strong interregional inequalities, which are likewise replicated in terms of data capacities. For example, according to the aforementioned NIC.br study, 168 of the 465 private data centers in Brazilian territory are located in the state of São Paulo[18]; furthermore, it is estimated that approximately half of new data-center investments in Brazil are channeled to the South and Southeast regions[19]. This concentration has direct implications for how much each region can benefit from such capacities, not only in terms of data processing itself, but also in terms of a potential increase in income resulting from a process of economic spillover.

In light of the foregoing, it is clear that the challenges faced by Brazil in building and leveraging data capacities are not only strongly interrelated but also mutually reinforcing. The lack of adequate infrastructure generates external dependencies, making Brazil's ownership and management of its own data vulnerable, reinforcing the traditional international division of labor in the digital environment, and consequently reducing the benefits the country could obtain from its data. Similarly, low profit-generating capacity hinders investment in infrastructure, thereby consolidating a cycle of deepening asymmetries.

Therefore, the challenges faced by Brazil are multidimensional and interdependent. The ANPD, in coordination with other government bodies and international partners, has been working to mitigate these challenges, promoting a regulatory environment that reconciles personal data protection with innovation and economic development.

Ministry of Health (MS)

Brazil faces challenges related to technological infrastructure, data management, quality and standardization, and interoperability and integration among health information systems. Heterogeneities persist among the Union, states, municipalities, and the Federal District regarding digital infrastructure, connectivity, processing capacity, and institutional maturity for data governance, which limits full integration of local systems into the National Health Data Network (RNDS).

The fragmentation of information systems, the coexistence of legacy systems — such as the SUS Hospital Information System (SIH/SUS), the SUS Outpatient Information System (SIA/SUS), the Mortality Information System (SIM), and the Live Birth Information System (SINASC) — differing technological standards, the lack of homogeneity among integrators' specialized teams, and the multiplicity of frontline systems where care is actually delivered, hinder governance, interoperability, and data sharing at the national scale, in addition to contributing to challenges related to incomplete integration and data quality, compromising longitudinal and predictive analyses. Although the country has relevant regulatory frameworks and digital infrastructures, asymmetries persist among federative entities and institutions regarding their capacity to produce, share, and use data interoperably.

Added to this is the complexity of the Brazilian federative model, in which municipalities produce and manage most of the data, states carry out partial consolidation, and the Union coordinates national policies and seeks to centralize information through national systems and the RNDS, making robust shared governance mechanisms, semantic standardization, and data collection qualification essential. In the context of the growing use of data for research and innovation, including artificial intelligence applications in health, challenges remain regarding cross-border data flows and the operationalization of the safeguards provided for in the General Data Protection Law (LGPD), as well as the promotion of a more equitable distribution of the benefits arising from the use of this data, reducing asymmetries between the public and private sectors and expanding its use in the public interest.

2) How are inequalities embedded in the processes through which data is generated, collected and used in your country? In particular, how do biases in data collection and use, such as gender data gap, affect policymaking, service delivery and development outcomes? (Please provide examples, evidence and any measures being taken to address these disparities)

Ministry of Science, Technology and Innovation (MCTI)

Inequalities emerge from the very point of access. According to a 2024 report published by the Brazilian Network Information Center (NIC.br), only 22% of the Brazilian population has access to meaningful connectivity, while the majority accesses the internet under restrictive conditions through limited mobile data plans or arrangements relying on practices such as zero-rating. This constrains the productive use of connectivity, exacerbates inequalities, distorts competition, and limits the exercise of digital sovereignty. Furthermore, artificial intelligence systems trained on datasets that do not adequately reflect the diversity of the Brazilian population are likely to reproduce and perpetuate historical inequalities, particularly those related to race and gender. When training data are biased, automated decision-making in sensitive sectors, such as credit allocation, public security, and healthcare, may reinforce discriminatory outcomes. Moreover, the lack of specific data on minority groups, traditional communities, and gender-related issues — a phenomenon commonly referred to as the gender data gap — directly undermines the effectiveness of public policies. In the absence of granular, representative, and high-quality data, the State is less able to design policies that effectively address the needs of these populations, potentially resulting in development strategies that are less inclusive and more unequal. Against this backdrop, the Brazilian Artificial Intelligence Plan (PBIA), grounded in the principle of a human-centered approach to artificial intelligence, seeks to prevent discriminatory biases and promote cultural diversity. Among its key initiatives is the development of language models based on national datasets, with the objective of ensuring that the specific characteristics of Brazilian culture and its diverse social

groups are adequately represented, thereby reducing the reproduction of biases stemming from foreign datasets.

Ministry of Justice and Public Security (MJSP) — National Secretariat for Digital Rights, Data Protection Coordination-General

The LGPD establishes a strict protection regime for sensitive data, a category that includes racial or ethnic origin, religious belief, health-related data, sexual life, and genetic or biometric data. The processing of such categories is subject to specific authorizing hypotheses and the principle of non-discrimination, ensuring that data use occurs in an ethical and fair manner.

Brazil is attentive to the challenges inherent to automated data processing in credit systems, employment selection, and the granting of social benefits. The country has promoted in-depth discussions to ensure that the use of algorithms does not reproduce historical biases, ensuring that correlated variables do not function as proxies for sensitive categories.

The ANPD has been developing proactive guidance on the subject in the context of artificial intelligence regulation, in line with OECD recommendations and international best practices. Brazil also played a prominent role, during its 2024 G20 presidency, in the work of the Digital Economy Task Force (DETF) on AI governance and data protection.

The Brazilian government recognizes the importance of representative databases for the development of effective public policies. Institutions such as IBGE have continuously improved their methodologies to ensure inclusion and statistical accuracy, mitigating data gaps such as those related to gender and race, and ensuring that technological innovations benefit the entire population equitably.

The ANPD published, in 2024, a technical note on facial recognition in public spaces, addressing best practices for the use of this technology and the safeguards necessary to prevent bias. Promoting the representativeness of training data and the auditability of automated systems is a priority on the country's regulatory agenda.

The LGPD provides special protection for the processing of data of children and adolescents (Art. 14), requiring parental consent and prohibiting processing contrary to the best interests of the minor. The National Data Protection Authority has regulated this matter, with direct impact on streaming platforms, digital games, and social networks widely used by the young Brazilian population.

With regard to indigenous and quilombola populations, data collection in traditional territories raises questions about informational self-determination and collective data sovereignty — a topic still incipient in Brazilian regulation and one that deserves special attention in the context of international debates on data governance for development.

Data Processing and Information Technology Company for Social Security (Dataprev)

Inequalities manifest in the processes of data generation, collection, and use through informational gaps, coverage asymmetries, and unequal representativeness of certain population groups.

The incompleteness or low quality of data can compromise the formulation of public policies, particularly with regard to identifying vulnerable populations, impacting resource allocation and the effectiveness of government actions.

Additionally, the absence of data models sensitive to cultural and regional specificities can result in distortions in the representation of social and family identities, contributing to the perpetuation of biases.

Among the measures adopted to mitigate these distortions are initiatives for registry qualification, integration of administrative records, expansion of database coverage, and the establishment of information quality monitoring mechanisms, focusing on attributes such as completeness, consistency, accuracy, and timeliness.

National Data Protection Authority (ANPD)

In Brazil, social inequalities — especially those of gender, race, and income — are not only reflected in data but are embedded in the very processes of production, collection, and use of this information, generating direct effects on public policy formulation and development outcomes.

Regarding inequalities in data generation and collection, one of the main problems Brazil currently faces is the insufficiency of data disaggregated by gender, age, race and ethnicity, territory, income, and other relevant social markers. The absence of intersectional data analysis, in turn, makes it difficult to capture complex inequalities that involve different types of discrimination and result in particular vulnerability being imposed on certain social groups.

One example illustrating this analytical gap is how essential activities related to caring for children and the elderly are made invisible in public policies and remain socially and economically undervalued. One of the actions aimed at addressing this gap is DataCuidados, a strategic initiative of the National Secretariat for Care and Family Policy of the Ministry of Development and Social Assistance, Family and Fight Against Hunger (MDS), in partnership with the National School of Public Administration (ENAP) and the Oswaldo Cruz Foundation (Fiocruz). It is an interactive public dashboard of indicators that enables systematic and disaggregated visualization and analysis of the reality of care in Brazil.

In response to difficulties related to data and the effective realization of gender equality in the country, the Ministry of Women established, in 2009, the Brazil Gender Equality Observatory, a strategic mechanism to support the formulation and implementation of public policies for women in Brazil and to monitor gender inequality indicators and women's rights.

One of the Observatory's actions seeks to address another significant challenge in the country: the appropriate use of already-collected data for evidence-based policymaking. This is the Annual Socioeconomic Report on Women (RASEAM), an initiative that compiles approximately 320 indicators and more than 380 data tables on gender issues across Brazil. RASEAM is a publication that annually gathers information from multiple official sources on women, divided into: (i) Demographic Structure; (ii) Economic Autonomy and Equality in the Labor Market; Education; (iii) Comprehensive Health, Sexual and Reproductive Rights; (iv) Combating all forms of violence against women; (v) Women in Positions of Power and Decision-Making; and (vi) Women in Culture, Communication, and Sports. The Report aims to centralize data and serve as a strategic guide for the creation of public policies and the development of scientific research in the field of gender equality.

Still within the framework of the Brazil Gender Equality Observatory — and drawing on RASEAM's results — the Ministry of Women structured, in 2026, DataMulheres, an integrated digital platform that gathers data on the reality of women in Brazil, inspired by the aforementioned DataCuidados. The platform automates the processes of collecting, processing, integrating, and consolidating socioeconomic data that portray gender inequality in the country, enabling dynamic, customized analyses of statistics related to the gender agenda. It is aimed especially at public managers and researchers — its access is not yet open to the general public, requiring registration to use it.

It should also be noted that the production of gender-related public policies depends on the country's institutional capacities, which vary according to the resilience of state policies oriented toward gender equality across different federal, state, and municipal governments. In this sense, a pressing problem marking Brazilian reality is dealing with periods of weakening of policies for women and the discontinuity of programs designed to last for long periods, which is deepened during times of budget cuts and even loss of ministerial status for this agenda.

Regarding impacts on public policy formulation, it can be said that the absence of gender data and other social markers causes policies to be poorly calibrated or incomplete, impacting the efficient allocation of public resources and the effectiveness of these initiatives. Thus, access to more accurate, intersectional data enables the proper targeting of policies to those who need them most, as well as monitoring and evaluation of how the

public budget is implemented. Without effective public policies, in addition to poor allocation of public resources, there is a risk of deepening regional and social inequalities, affecting the country's development.

The absence of disaggregated and representative data can generate barriers to access to health, education, social assistance and protection services, as well as employment and income policies, resulting in the underservicing of vulnerable populations and the perpetuation of inequalities. Furthermore, insufficient data hinders the monitoring of outcomes, the identification of excluded groups, and the adoption of corrective measures to improve the effectiveness and equity of public policies.

It is also worth noting that structural racial inequalities are reflected in these processes, producing major impacts on public policy formulation and the guarantee of fundamental rights. An emblematic example is the use of facial recognition technologies in public security, which has been shown to reproduce and, at times, amplify historically existing racial biases.

Studies indicate that these systems present higher error rates for Black people, especially Black women, due to unrepresentative databases. This problem is aggravated in the Brazilian context, marked by racial inequalities and the growing adoption of these technologies by public bodies, still without sufficiently robust mechanisms for oversight, transparency, and accountability, especially in large urban centers, where millions of faces can be captured daily.

A survey by the Federal Public Defender's Office (DPU) and CESeC indicates that the country had, in 2025, at least 376 active facial recognition projects, with the potential to monitor about 40% of the population, with the majority of people identified in police stops being Black — reaching approximately 90% in some contexts. Concrete cases, recorded in states such as Sergipe and Bahia, show wrongful detentions of Black citizens due to false positives, including episodes of prolonged deprivation of liberty. This evidence demonstrates how algorithmic biases can affect fundamental rights and compromise the legitimacy of public security policies.

In response, Brazil has gradually advanced in building institutional and regulatory capacities. The ANPD has played an important role in guiding the processing of personal data. On this specific topic, as of May 2026, the ANPD has already adopted important measures, such as the publication, in June 2024, of Technology Radar No. 2, on biometrics, which highlights risks of discrimination and bias in automated systems; and, in 2025, it launched a public consultation for the regulation of biometric data use, including concerns about discriminatory impacts, transparency, and accountability.

Despite these advances, regulatory gaps persist, especially regarding specific rules for biometric surveillance technologies and the systematic adoption of algorithmic impact assessments.

As a lesson, the Brazilian case shows that data governance, especially in high-impact contexts, must incorporate a racial equity perspective, emphasizing: (i) data quality and representativeness; (ii) independent audits; (iii) system transparency; and (iv) effective remedy mechanisms.

Without these measures, there is a risk that digital transformation will reinforce historical inequalities rather than mitigate them.

Beyond racial and gender inequalities, the specificities of persons with disabilities in data processes also constitute a relevant challenge in Brazil. The country has approximately 14.4 million people with disabilities (7.3% of the population), but still faces gaps in data production, including underreporting and low disaggregation by type of disability and other social markers. These limitations also hinder effective public policies and reinforce this group's invisibility. Moreover, historical inequalities — such as illiteracy rates four times higher than those of the population without disabilities, for example — contribute to their underrepresentation in digital databases and data-driven systems.

In the context of service digitalization and the growing use of artificial intelligence, these inequalities may deepen. Digital platforms and automated systems do not always incorporate adequate accessibility standards, which can exclude people with disabilities from access to essential services and from the very generation of data on their needs. Additionally, AI-based systems may reproduce biases by failing to consider functional

diversity — for example, by failing to recognize speech, assistive navigation, or other forms of interaction. Although AI also offers potential to expand inclusion through assistive technologies, the Brazilian case shows the need to integrate accessibility, data governance, and inclusive design as central pillars of digital transformation.

Ministry of Health (MS)

The expansion of the National Health Data Network (RNDS) has clearly shown how structural, territorial, and institutional inequalities are embedded in the processes of data generation, collection, integration, and use in Brazil. Regional differences in technological infrastructure, connectivity, processing capacity, technical qualification, and information management capacity among integrating units result in asymmetries that directly impact the quality, availability, and scope of information used for public policy formulation. Small municipalities and regions with lower technological capacity face difficulties in collecting, updating, integrating, and sharing information, which compromises their full integration into the RNDS, may generate coverage gaps, and hinder comparative analyses and evidence-based decision-making processes.

8. In addition, the scarcity of professionals specialized in interoperability and data governance accentuates heterogeneity in adoption, creating a scenario in which large urban centers advance more quickly, while localities with lower administrative capacity face greater difficulties keeping pace with this process. These inequalities can be reflected in biases in data collection and use, impacting both public policy formulation and service delivery, which is subject to inconsistencies in the integration of local systems.
9. Recognizing these challenges, Brazil has adopted measures to address them. The SUS Digital Program provides technical support and training actions in municipalities with lower infrastructure. SEIDIGI has been promoting training for local managers and technicians, while the Ministry of Health and the Brazilian Institute of Geography and Statistics (IBGE) expand efforts to include gender, race, and territory variables in information systems. In parallel, federal connectivity expansion initiatives seek to reduce the digital exclusion that directly impacts the RNDS. Overcoming these asymmetries requires continuous investment in digital infrastructure, training and technical qualification, process standardization, strengthening of local information management capacities, disaggregated data collection, and federative and international cooperation, in order to ensure equitable and interoperable data governance that contributes to shared prosperity and sustainable development.

3) Has your country implemented national strategies, regulatory frameworks or policy instruments to promote equitable and interoperable data governance? What are the lessons learned? (Please describe any specific challenges, failures or successes encountered during implementation)

Ministry of Science, Technology and Innovation (MCTI)

Brazil's data governance framework is grounded in well-established legal instruments, including the Marco Civil da Internet (Law No. 12,965/2014) and the Lei Geral de Proteção de Dados Pessoais (Law No. 13,709/2018). In addition, the governance of artificial intelligence, as set out in the Brazilian Artificial Intelligence Plan (PBIA), is integrated into the country's Legal Framework for Science, Technology and Innovation, comprising Constitutional Amendment No. 85/2015, Laws No. 10,973/2004 and No. 13,243/2016, and Decree No. 9,283/2018, as well as industrial policy instruments, including the Lei de Informática (Information Technology Law, Law No. 8,248/1991) and Law No. 13,969/2019. The PBIA is guided by the principles of transparency, traceability, and accountability, while seeking to strengthen data sovereignty and cybersecurity. As part of its institutional and regulatory development, the Plan provides for the establishment of a national center dedicated to artificial intelligence risk management, safety, and trustworthiness. At the legislative level, discussions continue to advance through the consideration of Bill No. 2,338/2023 and Bill No. 2,688/2025. One of the key lessons learned is that the existence of a sound legal framework is a necessary, but not sufficient, condition for effective governance. Its successful implementation requires robust enforcement mechanisms and strong institutional coordination to prevent governance fragmentation.

Ministry of Justice and Public Security (MJSP) — National Secretariat for Digital Rights, Data Protection Coordination-General

The General Data Protection Law (LGPD), in force since September 2020, is Brazil's main regulatory instrument for personal data governance. Inspired by the European Union's General Data Protection Regulation (GDPR), the LGPD establishes: (i) the principles of data processing (purpose, adequacy, necessity, free access, quality, transparency, security, prevention, non-discrimination, and accountability); (ii) the legal bases authorizing processing; (iii) data subjects' rights; (iv) controllers' and operators' obligations; and (v) the sanctioning regime applied by the National Data Protection Authority.

The National Data Protection Authority, created as a special-nature autarchy with technical and decision-making independence and later elevated to regulatory agency status, plays a central role in infra-legal regulation, oversight, guidance, and coordination with international bodies. Starting in 2022, the National Data Protection Authority began its sectoral regulation cycle, issuing rules on: (i) international data transfer (CD/ANPD Resolution No. 19/2024); (ii) security incident reporting (CD/ANPD Resolution No. 15/2024); and (iii) protection of children's and adolescents' data.

In the context of the State's digital transformation, the National Data Infrastructure (IND), established by Decree No. 12,198/2024, represents a strategic project of great scope to organize, integrate, and standardize public administration databases. The initiative has driven improvements in public service delivery, ensuring privacy and fostering the ethical use of artificial intelligence.

Among the challenges identified in implementing the IND is the persistence of data silos across different federal bodies, the heterogeneity of information technology systems in the public sector, and the need to strengthen the data governance culture in state and municipal administrations, which often lack adequate technical structures.

Decree No. 10,046/2019 established the framework for data sharing within the federal Executive Branch, creating the Central Data Governance Committee (CCGD) and the Citizen's Base Registry. This instrument enabled advances in the interoperability of government databases, reducing the need for citizens to repeatedly provide the same data across different public services.

The MJSP Data Governance Policy (MJSP Ordinance No. 2/2022) established guidelines for data processing and sharing, in compliance with the LGPD, serving as a good-practice model for the federal public administration.

Brazil's experience implementing the LGPD has generated valuable lessons:

- The consolidation of a strong and independent regulatory Authority is fundamental to the effectiveness of the legal framework;
- Synergy between data protection and open data policies has promoted an environment of legal certainty and innovation;
- Engagement from civil society and the private sector has been essential to building a culture of privacy in the country;
- The regulation of new technologies, especially artificial intelligence and algorithmic scoring systems, needs to be incorporated into the data protection framework in an agile manner, avoiding regulatory gaps that perpetuate power asymmetries.

Data Processing and Information Technology Company for Social Security (Dataprev)

Brazil has a structured regulatory framework for data governance, composed, among other instruments, of:

- Law No. 13,709/2018 (General Data Protection Law — LGPD);
- Decree No. 10,046/2019, which provides for data-sharing governance within the Federal Public Administration;
- Law No. 14,129/2021 (Digital Government Law);

- 2024–2027 Federal Digital Government Strategy;
- Open Data Policy (Decree No. 8,777/2016).

On the operational front, the Conecta gov.br Platform stands out, enabling data sharing through standardized interfaces, ensuring technical interoperability, access control, traceability, and compliance with information security requirements.

Among the main lessons from implementing these instruments, the importance of technical and semantic standardization, centralized coordination with decentralized execution, metadata management, and the adoption of open standards that mitigate risks of technological dependence stand out.

National Data Protection Authority (ANPD)

The LGPD enshrines principles, guarantees rights to data subjects, and imposes duties on processing agents, demonstrating that any interoperability and data-sharing initiative must be designed and implemented in strict compliance with personal data protection. Beyond the LGPD, there is a legal framework that underpins this governance and data sharing within the federal public administration, which reflects an ongoing effort to build a comprehensive regulatory architecture to promote secure sharing and the responsible use of data.

Thus, equitable and interoperable data governance in Brazil rests on the General Data Protection Law (LGPD), which enshrines principles, data subjects' rights, and processing agents' duties, and demonstrates that data governance and interoperability cannot be dissociated from personal data protection, and must be implemented in strict compliance with this framework.

Beyond the LGPD, it is worth mentioning other instruments that structure data governance in the country — particularly the Digital Government Law (Law No. 14,129/2021) and the Marco Civil da Internet (Law No. 12,965/2014) — as well as decrees and ordinances related to digital transformation and data sharing within the federal public administration; the next question provides an informative list of these legal instruments. Mentioning this regulatory set demonstrates that Brazil is building a comprehensive regulatory architecture to enable secure sharing, interoperability, and responsible data use.

In any case, within the ANPD's competencies, no regulatory frameworks have been implemented with the specific objective of promoting equitable and interoperable data governance. Nonetheless, it is worth highlighting the effects generated by the International Data Transfer Regulation (RITCD, cited in the previous question), which establishes rules aimed at enabling cross-border data flows with trust. Based on these rules, the ANPD recently recognized the European Union as a jurisdiction with a level of data protection equivalent to national legislation, simplifying the data transfer process between Brazil and Europe.

Ministry of Health (MS)

Brazil has a robust set of regulatory instruments and public policies aimed at promoting secure, interoperable data governance oriented toward the public interest. Notable instruments include Law No. 13,709/2018 (General Data Protection Law — LGPD), which establishes principles and guarantees for personal data processing; Law No. 12,965/2014 (Marco Civil da Internet), which defines the foundations of the Brazilian digital environment, including privacy and personal data protection; Law No. 14,129/2021 (Digital Government Law), which encourages the digital transformation of Public Administration, interoperability among systems, and data sharing to improve public services; and Decree No. 10,046/2019, which established data-sharing governance within the Federal Public Administration. In the health sector, notable instruments include the SUS Digital Program, established by Ordinance GM/MS No. 3,232; the National Health Data Network (RNDS), officially established as the SUS interoperability platform through Decree No. 12,560/2025; and the Ministry of Health's Open Data Plan, grounded in Decree No. 8,777/2016, which established the Federal Executive Branch's Open Data Policy. These frameworks promote interoperability, standardization, and health information sharing.

11. In addition, the Brazilian Digital Government Strategy (Decree No. 10,332/2020) drives the integration and digitalization of public services. Institutionally, the Ministry of Health also has specific instruments that strengthen digital and data governance. Ordinance SE No. 518, of November 5, 2021, establishes guidelines for the

development of new ICT solutions, determining that new system demands be preceded by studies prioritizing data integration and the reuse of existing solutions, contributing to reducing informational fragmentation, rationalizing investments, and strengthening interoperability.

12. Additionally, Ordinance GM/MS No. 7,678, of July 23, 2025, which establishes the Strategy for the Use of Software and Cloud Computing Services within the Ministry of Health, sets guidelines related to data governance, information security, personal data protection, interoperability, data sovereignty and residency, risk management, transparency, and modernization of digital infrastructure, as well as providing for formal evaluation, monitoring, and decision-making mechanisms. The implementation of this regulatory framework has produced significant advances in the integration of digital systems and services, in the modernization of public management, in strengthening information security, and in expanding the capacity to use data for development.
13. Among the main lessons learned are the importance of clear federative governance, inter-institutional coordination, process standardization, and the adoption of interoperable standards, including the progressive implementation of HL7 FHIR, as well as the recognition that technical training is as important as technology investments. However, challenges remain related to institutional adaptation, system fragmentation, the low digital maturity of some federative entities, difficulties in adoption in localities with lower technical capacity, and the long-term financial and operational sustainability of digital initiatives.

4) Can you share your country's experience in reducing asymmetries and promoting more equitable data stewardship in development sectors such as public services, education, health and agriculture? (Please provide examples, lessons learned and remaining challenges where possible)

Ministry of Science, Technology and Innovation (MCTI)

Brazil's experience in promoting equitable data governance and reducing sectoral asymmetries is reflected in the Brazilian Artificial Intelligence Plan (PBIA), which prioritizes the development of technologies aimed at advancing social well-being and strengthening national sovereignty. To this end, the PBIA comprises a set of immediate-impact and structural initiatives spanning a broad range of strategic sectors that are essential to the country's development and well-being. With regard to its structural initiatives, which are designed to strengthen national sovereignty, technological autonomy, competitiveness, sustainable innovation, and the responsible and ethical adoption of artificial intelligence in Brazil, the Plan is organized around five strategic pillars: 1) AI Infrastructure and Development; 2) AI Diffusion, Education, and Capacity Building; 3) AI for the Improvement of Public Services; 4) AI for Business Innovation; and 5) Support for the AI Regulatory and Governance Framework. Overall, the PBIA comprises 54 structural initiatives, the implementation and monitoring of which can be followed through the digital platform of the Brazilian Artificial Intelligence Observatory (OBIA), available at <https://obia.nic.br/s/indicadores-pbia>, as well as through the PBIA website, available at <https://pbia.cgee.org.br/sobre/>.

Ministry of Justice and Public Security (MJSP) — National Secretariat for Digital Rights, Data Protection Coordination-General

Gov.br, the federal government's unified digital services platform, consolidates access to more than 4,000 public services through a unified digital identity. From a data protection perspective, the LGPD fully applies to the processing of personal data on this platform, requiring compliance with the principles of necessity, purpose, and security. The Gov.br model has helped reduce access asymmetries by eliminating the need for in-person travel and paperwork.

The ANPD and the Ministry of Management and Innovation in Public Services (MGI) maintain a strategic partnership to ensure that the ongoing expansion of the Brazilian State's digital services is guided by best practices in data protection and governance.

Regarding information related to Health, Education, and Agriculture, on the promotion of data management in public services, these questions should be addressed and directed to the respective ministries.

Data Processing and Information Technology Company for Social Security (Dataprev)

The adoption of interoperability mechanisms has produced significant results in different areas of Public Administration:

- **Social assistance:** improved beneficiary identification, reduced inconsistencies, and greater efficiency in managing the Single Registry (Cadastro Único);
- **Health:** strengthened integration of records and improved epidemiological surveillance;
- **Education:** enabling the tracking of educational trajectories and supporting school-retention policy formulation;
- **Labor and social security:** greater speed and reliability in benefit-granting processes.

These advances demonstrate the role of interoperability as an instrument for increasing administrative efficiency, improving data quality, and supporting evidence-based public policymaking.

National Data Protection Authority (ANPD)

Data governance in Brazil is grounded in the LGPD, which enshrines principles, grants rights to data subjects, and imposes duties on processing agents, demonstrating that interoperability and shared data-use initiatives must be designed and operationalized in strict compliance with personal data protection. Beyond the LGPD, the regulatory framework structuring this governance includes:

- Law on incentives for innovation and scientific and technological research in the productive environment (Law No. 10,973/2004);
- Access to Information Law (Law No. 12,527/2011);
- Marco Civil da Internet (Law No. 12,965/2014);
- The decree coordinating data sharing among federal Executive Branch bodies and establishing the Citizen's Base Registry and the Central Data Governance Committee (Decree No. 10,046/2019);
- Digital Government Law (Law No. 14,129/2021);
- Data-sharing governance (Decree No. 11,266/2022);
- National Digital Government Strategy (Decree No. 12,069/2024); and
- Digital Citizenship Platform, providing for the offer of digital public services (Decree No. 8,936/2016).

Together, these instruments indicate a progressive effort to build a comprehensive regulatory architecture that seeks to promote secure sharing, technical and semantic interoperability, and responsible data use, while preserving fundamental rights and promoting trust in the digital space.

Brazil's experience in promoting more equitable data management and reducing asymmetries offers a relevant set of practices, especially in data-driven public policy. Regarding public services and social protection, notable is the Single Registry (Cadastro Único), an integrated database that identifies low-income families and underpins income-distribution policies such as Bolsa Família. Another example, as mentioned earlier, is DataMulheres, a platform that consolidates disaggregated data to support gender-sensitive public policies. Such initiatives promote the ability to identify territorial and socio-demographic inequalities.

Regarding education, the School Census and the Higher Education Census are examples of comprehensive databases that monitor access and educational retention, supporting initiatives aimed at expanding access to education for historically excluded groups, especially the Black and low-income population, improving educational equity.

Regarding health data, DATASUS is a database that provides information supporting objective analyses of the country's health situation, ensuring that decisions are evidence-based, particularly in the design and

implementation of health action programs. One example of how this policy works in identifying inequalities is the fact that higher mortality from preventable causes is observed among the Black population.

In agriculture and rural development, the Agricultural Census can be cited, which contains data and records on rural credit and family farming policies, such as the National Program for Strengthening Family Farming (PRONAF) and the Food Acquisition Program (PAA). Such public policies can identify production profiles, differentiating, for example, small-scale actors from large producers, and identify regional inequalities, promoting support for food security and regional development.

The promotion of more equitable data management has advanced through institutional and regulatory initiatives still under consolidation. The National Data Protection Authority has produced guidance, guides, technical studies, and adopted instruments such as regulatory sandboxes and public consultations, which have made it possible to explore more flexible and participatory approaches to regulating emerging technologies, contributing to institutional capacity-building and the incorporation of fundamental-rights perspectives into data governance.

Finally, in parallel, Brazil has a consolidated track record in open government data policies, with initiatives such as the Brazilian Open Data Portal, which aim to expand transparency, data reuse, and social oversight, in addition to centralizing and making information available for consultation. However, challenges remain regarding the quality, standardization, and disaggregation of such data, especially regarding social breakdowns. Experiences with more advanced models of collective data governance, such as data trusts or data commons, are still incipient in the country, but are beginning to emerge in academic and regulatory debate, signaling the potential for structures that favor a more equitable distribution of benefits and greater social control over data use.

Ministry of Health (MS)

Brazil's experience in reducing informational asymmetries and promoting more equitable data management has materialized significantly through national infrastructures such as the National Health Data Network (RNDS) and the National Registry of Users of the Unified Health System (CadSUS). The RNDS has enabled data from different care events to be integrated and made available uniformly across the national territory, expanding access to, quality of, and use of health information. CadSUS, through the National Health Card (CNS), enables the unique identification of citizens, facilitating the integration of information from different health systems and facilities, reducing registration inconsistencies and duplication, and strengthening interoperability among systems. As part of this process, initiatives for registry qualification and integration with reference government databases stand out, particularly the Individual Taxpayer Registry (CPF) database, which increase the reliability, integrity, and traceability of information used in service delivery and public policy formulation.

15. For citizens, the benefits are concrete. Through Meu SUS Digital, each person can access their own health data, such as vaccination history, test results, and care records. This direct access strengthens users' autonomy, expands their participation in care decisions, and supports continuity of care, since information from different moments and services becomes available in an integrated way, reducing duplicate procedures and promoting greater clinical safety. National data integration was particularly evident during the COVID-19 vaccination campaign, demonstrating important advances in interoperability and large-scale information-sharing capacity.
16. For health professionals, the SUS Digital Professional platform offers structured access to integrated RNDS data, enabling a more comprehensive view of patient history, contributing to more accurate diagnoses, more appropriate treatment plans, and greater efficiency in service delivery. Interoperability between local and national systems strengthens continuity of care and helps reduce inequalities arising from differing infrastructure capacities across regions.
17. In terms of public management, the federalization of the RNDS and the existence of a standardized national user-identification database allow managers to access consistent information for planning, monitoring, and evaluating public policies. Municipalities with lower technical capacity benefit from nationally structured data, helping to reduce regional asymmetries, strengthen equity in policy formulation, and improve resource allocation.

Additionally, expanded registry coverage and improved record quality favor the production of more reliable information on access to health services, use of the care network, and the profile of the population served.

18. Among the main lessons learned are the importance of adopting reliable identifiers, registry standardization, interoperability among databases, transparency, and coordination among different public and private actors. Brazilian experience also demonstrates that data governance requires continuous investment in digital infrastructure, professional training, and record linkage and qualification, as well as ongoing system-integration processes. Remaining challenges include heterogeneity in integration capacity among federative entities, data quality and completeness, multilevel governance, continuous improvement of interoperability, timely updating of information, and ensuring the safe secondary use of data for research, through qualification, linkage, and anonymization mechanisms that preserve the identity, intimacy, privacy, and security of SUS users.
19. In summary, Brazilian experience demonstrates that the combination of national identification and interoperability infrastructures — represented by CadSUS and the RNDS — together with registry-qualification and data-integration mechanisms, helps reduce informational asymmetries, strengthen patient-centered care, promote greater efficiency in public management, and support the formulation of more inclusive, equitable, and evidence-based public policies.

5) What mechanisms or institutional arrangements are in place in your country to foster collaboration around data governance for development among different stakeholders (e.g., university-industry, private-public, or multi-stakeholder initiatives)?

Ministry of Science, Technology and Innovation (MCTI)

Brazil has established an institutional framework for data and artificial intelligence governance based on a multi-stakeholder and collaborative approach that brings together the public sector, academia, industry, and civil society. The Brazilian Artificial Intelligence Plan (PBIA) reflects this collaborative model, having been developed with the active participation of 117 institutions representing a broad range of stakeholders. The governance of the Internet and cross-cutting digital issues is supported by the Brazilian Internet Steering Committee (Comitê Gestor da Internet no Brasil — CGI.br), which serves as one of the country's principal multi-stakeholder governance bodies. CGI.br brings together representatives from different sectors to establish strategic guidelines and coordinate Brazil's participation in international Internet governance and standard-setting processes. More recently, this collaborative model has been further strengthened through the establishment of the Brazilian Artificial Intelligence Observatory (Observatório Brasileiro de Inteligência Artificial — OBIA), an initiative developed jointly by the Federal Government and CGI.br to monitor Brazil's artificial intelligence ecosystem and support evidence-based policymaking. Collaboration among universities, research institutions, industry, and government is also promoted through strategic initiatives under the PBIA. One notable example is Action 42 — Systemic Support for the AI Value Chain, which seeks to expand Brazil's capacity to develop artificial intelligence solutions for strategic challenges, strengthen cooperation among academia, the private sector, and government, and accelerate technology transfer, thereby contributing to the country's innovation capacity in artificial intelligence. In addition, the PBIA promotes the establishment of national institutes of science and technology in artificial intelligence (INCT-IA) and research networks in strategic areas, with the objective of strengthening national capabilities in science, technology and innovation, while fostering talent development, attraction, and retention.

Ministry of Development, Industry, Trade and Services (MDIC)

In 2024, MDIC proposed PBIA Action 49, aimed at structuring and executing a pilot data space project for Brazilian industry. This action is related to the National Data Economy Policy (PNED), since data spaces are a technological solution that enables the secure sharing of data.

Over recent months, MDIC has finalized the draft terms of reference related to Action 49. The use case selected for application in the Action 49 data space was the optimization of Research, Development, and Innovation

(RD&I) project development selected under the Smart Factory calls, which make up Modality IV of the Brazil More Productive Program (B+P). Action 49 has a projected value of R\$28 million. MDIC has been working and coordinating with MCTI and the Presidency's Council for Sustainable Economic and Social Development ("Conselhão") to enable faster contracting of this project, which will be financed with FNDCT resources.

Ministry of Justice and Public Security (MJSP) — Information and Communication Technology Sub-Secretariat

A relevant institutional mechanism in place at MJSP is the work of the Data and Information Systems Governance Committee (CGDI), which brings together representatives from all of the Ministry's state secretariats and affiliated bodies on a monthly basis, making the establishment of Technical Cooperation Agreements between MJSP and other bodies at the municipal, state, and federal levels — whose purposes include the sharing and/or significant production of data assets — dynamic and transparent. By June 2026, 282 databases had been catalogued.

Another relevant institutional mechanism, though one that still requires improvements and practices that induce and accelerate the sufficiency of data management and governance processes beyond processing within the CGDI, is the signing of Terms of Accession to the BRASIL M.A.I.S. Program (Integrated and Secure Environment). This is a strategic initiative that democratizes access to high-resolution satellite imagery and automatic alerts on deforestation, illegal mining, and fires for public institutions, which has already reached the possibility of access to more than 800 databases by MJSP through Federal Police coordination, under 1,050 Terms of Accession formalized by the 73rd Ordinary Meeting of the CGDI.

Both the Technical Cooperation Agreements and the Terms of Accession to BRASIL M.A.I.S. have their metadata catalogued by CGDAD, which acts as the Data Governance Office (EGD), with the exception of instruments subject to confidentiality or restriction. However, expansion of competencies and functional structures is needed so that, working jointly with the substantive units, it becomes possible to foster the use of these data assets, through data intelligence solutions serving public policies on justice and public security.

Ministry of Justice and Public Security (MJSP) — National Secretariat for Digital Rights, Data Protection Coordination-General

Brazil has a robust and participatory institutional architecture for data governance. The ANPD has the National Council for Personal Data and Privacy Protection (CNPD), a consultative body with multisectoral composition bringing together representatives from government, civil society, academia, and the business sector. This model ensures that public policy formulation is plural and representative.

The CNPD has stood out as a forum of excellence for multistakeholder debate, enriching the regulatory agenda with diverse perspectives and promoting an environment of constructive collaboration across all sectors of society.

The CCGD, established by Decree No. 10,046/2019, coordinates data-sharing governance within the federal Executive Branch. It is an intergovernmental mechanism that seeks to harmonize the different systems and databases of federal bodies, facilitating interoperability without compromising personal data protection.

SEDIGI maintains ongoing dialogue with research centers, academic groups specializing in data protection and digital rights, and representatives of the business sector, particularly technology-sector associations, through public consultations, thematic working groups, and training events.

The ANPD's Data Protection Education Program (PEPD) is a high-impact initiative that, in partnership with universities and professional associations, has disseminated a culture of data protection throughout the country.

Data Processing and Information Technology Company for Social Security (Dataprev)

Data governance in Brazil is enabled by institutional arrangements that promote coordination among different bodies and levels of government. Noteworthy are:

- The Central Data Governance Committee (CCGD), responsible for defining guidelines and parameters for data sharing within the Federal Public Administration;
- The integrated action of institutions such as DATAPREV, INSS, the Ministry of Social Security, and the Ministry of Development and Social Assistance;
- Partnerships with training institutions, such as the National School of Public Administration (ENAP);
- Initiatives within the open-data ecosystem and federative cooperation.

These mechanisms strengthen interoperability, standardization, and secure information sharing.

National Data Protection Authority (ANPD)

In Brazil, the multisectoral arrangements that today underpin data governance have been built over decades, through ongoing dialogue involving government, the business sector, the scientific and technological community, and civil society. The country developed a multisectoral matrix in its digital governance even before the data protection framework, which was later transposed to this field.

An example of this format is the Brazilian Internet Steering Committee (CGI.br), created in 1995 and reorganized by Decree No. 4,829/2003. It is an important reference for multisectoral internet governance. Its twenty-one councilors are distributed among government, the business sector, the third sector, and the scientific and technological community, with a non-governmental majority and decisions made by consensus. In 2009, it approved the Ten Principles for the Governance and Use of the Internet — which addresses standardization and interoperability — which inspired both the Marco Civil da Internet and the LGPD. Its operational arm, NIC.br, produces, through Cetic.br, the indicators that underpin evidence-based governance.

Additionally, the National Council for Personal Data and Privacy Protection (CNPD) — the ANPD's consultative body, provided for in the LGPD (Arts. 58-A and 58-B) — is the country's main multisectoral data-protection forum. It brings together twenty-three full councilors, and an equal number of alternates, appointed by the President of the Republic: alongside government seats, there are seats filled through selection processes and shortlists, from civil society, scientific and technological institutions, trade union confederations, and the business and labor sectors. Its role is to propose guidelines for the National Data Protection Policy, support the ANPD's work, and promote studies, debates, and public hearings.

Beyond these collegiate bodies, consultations, calls for input, and public hearings are mandatory practice in the national regulatory process, making the consultation of academia, the private sector, and civil society a routine — not exceptional — step in rule-making.

Collaboration in Brazil is not limited to advisory forums; it is also structured as shared regulatory experimentation. The AI and Data Protection Regulatory Sandbox, designed by the ANPD and established by Notice No. 2/2025, in cooperation with UNDP, brings together the regulator, technology companies, academia, and civil society to test, under supervision, AI systems that process personal data. In it, USP was selected as a technical partner, and up to three pilot projects remain under testing until the end of 2026 — an example of co-regulation, not merely ex post regulation.

There are also experimental environments run by other regulators — sandboxes maintained by the Central Bank, the Securities and Exchange Commission (CVM), and the Superintendency of Private Insurance (SUSEP), which test innovations in controlled dialogue with the regulated sector.

The reference in the question to university-industry initiatives finds, in the country, a consolidated legal basis and ongoing examples, namely:

Legal Framework for Science, Technology and Innovation (CT&I) and EMBRAPII — Constitutional Amendment No. 85/2015 and Law No. 13,243/2016 (which reformed the Innovation Law, Law No. 10,973/2004) underpin cooperation between research institutions and the productive sector; EMBRAPII operationalizes this, linking institutes and industry in the development of applied solutions.

- a) **Federal Government AI Nucleus** — Established under the Brazilian Artificial Intelligence Plan (PBIa), bringing together the Ministry of Management, the Civil House, MCTI, ENAP, Serpro, Dataprev, Finep, and UnB to develop solutions and build capacity for AI use over public data.
- b) **GO FAIR Brazil Agro** — Network coordinated by Embrapa, with collegial management involving UFRRJ, USP, and Unipampa, for the governance and reuse of agricultural research data according to FAIR principles (findable, accessible, interoperable, and reusable); it brings together more than forty public and private institutions.
- c) **INSPIRE Program (Finep/CPQD)** — Union partnership with CPQD, financed by Finep and FNDCT (R\$390 million over four years) under the PBIa, dedicated to research and development in AI and secure data processing for public services.
- d) **Open Finance** — Financial data-sharing ecosystem built jointly by the Central Bank and the market (financial institutions and fintechs), with shared governance and technical standards; it combines effective interoperability with data-subject control over their own data, through consent.
- e) The **National Data Infrastructure (IND)** systematizes rules, standards, and tools for the strategic and interoperable use of federal government data.

Taken together, these arrangements reveal a national characteristic of combining consultative and deliberative multisectoral bodies — led by CGI.br and CNPD — with regulated sectoral arrangements, co-regulation instruments, and innovation incentives. The CGI.br model, in particular — multisectoral, with a non-governmental majority and consensus-based decisions — is frequently cited as an international best practice for inclusive governance, aligned with the equitable-management approach guiding this CSTD topic.

This is not, however, a system free of tensions: civil society's still-limited capacity to participate in specialized technical forums, and the resource asymmetry between large technology companies and small national actors, remain concrete obstacles to truly equitable governance. Overcoming them requires strengthening the arrangements described here.

Ministry of Health (MS)

Brazil has multisectoral institutional arrangements that reinforce data governance and promote integration among different public and private actors. Notable is the Brazilian Internet Steering Committee (CGI.br), which acts as a space for participatory, multisectoral governance, in addition to public-private partnerships aimed at interoperability in digital health and cooperation initiatives among universities, government, and the productive sector for applied research. Within the Unified Health System (SUS), governance spaces at the federative level also deserve mention, especially the tripartite bodies involving the National Council of Health Secretaries (CONASS) and the National Council of Municipal Health Secretariats (CONASEMS), which contribute to dialogue among different levels of management and to building shared solutions.

- 21. Also notable are initiatives aimed at strengthening information quality, interoperability, and data governance, with CadSUS as the main example. To ensure registry quality and the unique identification of citizens, CadSUS operates through institutional arrangements involving integration with strategic government databases, including the Brazilian Federal Revenue Service for validation of data associated with the Individual Taxpayer Registry (CPF), the National Civil Registry Information System (SIRC), which contributes to updating vital events, and services made available through the Conecta GOV.BR platform, including APIs related to Persons with Disabilities and Labor Relations.
- 22. Another relevant example is the National Data Infrastructure (IND), coordinated by the Ministry of Management and Innovation in Public Services (MGI), which contributes to secure sharing and the strategic use of data in the public sector. This arrangement fosters interoperability among different government databases and promotes

coordination among bodies responsible for producing, managing, and using data, strengthening digital governance and the integration of public policies across different sectors, including health.

23. In the health sector, collaboration around data governance is also strengthened by institutional coordination and participation mechanisms, such as the Digital Health Governance Committee (CGSD) and the National Health Council's Technical Chamber for Digital Health and Health Communication (CTSDCS/CNS), which bring together government representatives, regulatory bodies, and civil-society actors to discuss standards, interoperability, data protection, and digital transformation strategies. In addition, cooperation agreements with institutions such as the National Education and Research Network (RNP) and the Brazilian Network Information Center (NIC.br) contribute to producing evidence, technical cooperation, and strengthening institutional capacities related to data governance.
24. These cooperation mechanisms increase the reliability, integrity, and quality of information, reduce registration inconsistencies, strengthen record-qualification processes, and promote greater interoperability among government databases. They also contribute to more efficient use of public data, avoiding redundancy, strengthening integration between policies and digital services, and expanding the capacity for formulating, monitoring, and evaluating evidence-based public policies.
25. Brazilian experience shows that data governance for development depends on continuous coordination among institutions responsible for producing, managing, and using data, the adoption of interoperable standards, and mechanisms enabling secure, responsible, and efficient information sharing among different government systems. These experiences show that multisectoral cooperation, federative coordination, and database integration are fundamental elements for strengthening digital governance, data quality, and the delivery of more efficient public services centered on the population's needs.

6) What major bilateral, regional, or international partnership has your country engaged in to foster equitable and interoperable data governance? (Please describe the benefits of participating in these partnerships, as well as any challenges related to coordination, capacity, trust, interoperability or benefit-sharing)

Ministry of Science, Technology and Innovation (MCTI)

Brazil's international engagement in data and artificial intelligence governance is guided by a strategic vision that seeks to balance the strengthening of national capabilities with active and meaningful participation in global governance regimes, based on the principles of equity, cooperation, and mutual benefit. As established in the Brazilian Artificial Intelligence Plan (PBIA), Brazil views international cooperation as an essential dimension of sovereignty, aimed at ensuring that technological progress contributes to human development and to the protection of information integrity at the global level. In this context, technical and scientific cooperation constitutes a central pillar of the national strategy. The PBIA promotes research and development partnerships, particularly with countries in Latin America, the Caribbean, and Africa. This South-South cooperation strategy seeks not only to facilitate access to and the sharing of Brazil's research infrastructure, but also to strengthen the country's role in representing the interests and priorities of developing countries in discussions on the formulation of international norms and standards. It is also important to note that, while international partnerships offer significant benefits, including the reduction of asymmetries and the mitigation of technological dependencies, they also present the challenge of addressing weaponized interdependence by mitigating the risks associated with panoptic effects and critical chokepoints arising from foreign control over critical infrastructure. In this regard, Brazil's digital diplomacy seeks to promote the incorporation of safeguards within international governance frameworks against the coercive use of technological dependencies, while fostering an open, transparent, and auditable innovation environment that reinforces informational self-determination and the right to development on the basis of mutual benefit.

Ministry of Development, Industry, Trade and Services (MDIC)

Brazil-Germany Digital Dialogue: Under the coordination of the Ministry of Science, Technology and Innovation (MCTI), this partnership comprises a set of initiatives and agreements aimed at strengthening cooperation in various areas, including technology, infrastructure, and governance. The partnership promotes the exchange of experiences aimed at development and innovation in the digital field. The initiative is already underway and, on the Brazilian side, involves several bodies such as the Civil House, the Ministry of Foreign Affairs (MRE), and MDIC. On the European side, the main counterpart is the Directorate-General for Communications Networks, Content and Technology (DG CNECT). The joint agenda covers strategic topics such as artificial intelligence, digital platforms, digital markets, and electronic signatures, among others.

Brazil-European Union Digital Dialogue: MDIC has a partnership with GIZ (Deutsche Gesellschaft für Internationale Zusammenarbeit) aimed at developing and promoting the data economy in Brazil to support the drafting of the National Data Economy Policy. The project was structured around three pillars: i) hiring consultants, ii) a technical mission to Europe, and iii) technical workshops in Brazil. GIZ hired consultants to prepare two studies — one on the data market in Brazil and another on legal recommendations based on the European Union's experience with data. The DEIN team participated in a technical mission to Europe, held in November 2025, with visits to the European Commission and selected Member States focused on technical exchange on data governance measures. Regarding the dissemination of the PNED in Brazil, representatives of the European data space (Gaia-X) visited Brazil in November 2025, there was engagement with Brazilian and European parliamentarians, and finally a technical workshop was held at MDIC on March 31, 2026, with the participation of EU authorities and representatives of the Brazilian government to present and disseminate the results of the call for input for the PNED and partial results of the contracted consultancies.

Ministry of Justice and Public Security (MJSP) — Information and Communication Technology Sub-Secretariat

As already mentioned, we report the establishment of partnerships through Technical Cooperation Agreements between MJSP and other bodies at the municipal, state, and federal levels, whose purposes include the sharing and/or significant production of data assets. By June 2026, 282 databases had been catalogued.

Another relevant institutional mechanism for partnerships is the signing of Terms of Accession to the BRASIL M.A.I.S. Program (Integrated and Secure Environment), a strategic initiative that democratizes access to high-resolution satellite imagery and automatic alerts on deforestation, illegal mining, and fires for public institutions, which has already reached the possibility of access to more than 800 databases by MJSP through Federal Police coordination, under 1,050 Terms of Accession formalized by the 73rd Ordinary Meeting of the CGDI.

Ministry of Justice and Public Security (MJSP) — National Secretariat for Digital Rights, Data Protection Coordination-General

Brazil deeply values international cooperation as an instrument for strengthening global data governance. The European Union is one of the strategic partners, given that the GDPR served as a reference for the LGPD. Brazil has maintained productive dialogues aimed at mutual recognition of the adequacy of their regulatory frameworks, which will boost digital trade and economic integration between the regions.

The country has demonstrated the high level of maturity of its legislation and the independence of its National Authority, working collaboratively to align understandings and facilitate cross-border data flows for the benefit of both economies.

Brazil has a prominent role in the Ibero-American Data Protection Network (RIPD), actively contributing to the exchange of experiences and regulatory harmonization in the region. Brazilian participation has strengthened cooperation ties in Latin America and the Iberian Peninsula, promoting capacity-building and the construction of a dynamic and integrated regional data protection space.

Among the challenges are differences in institutional capacity among member authorities, the heterogeneity of national legal frameworks, and the absence of binding cooperation mechanisms for cross-border incidents.

Within Mercosur, Brazil has led efforts toward regulatory harmonization, understanding that digital integration is a fundamental pillar for the bloc's economic and social development.

During Brazil's 2024 G20 presidency, SEDIGI monitored the work of the Digital Economy Task Force (DETF), which addressed AI governance, data protection, and cross-border flows. The Brazilian presidency sought to incorporate the perspective of developing countries, including the issue of data asymmetry and digital sovereignty, into the group's outcome documents, with partial success given the difficulty of reconciling divergent positions among major digital powers.

Brazil also monitors the OECD's work on Artificial Intelligence and data governance, having adhered to the OECD's AI Recommendation (2019). Brazil's OECD accession process represents an opportunity to align the national regulatory framework with international standards, but also poses challenges of adapting rules built predominantly by developed countries to Brazilian reality.

Brazil has developed bilateral technical cooperation with Lusophone African countries and Latin American countries that are building or improving their data protection frameworks. This South-South cooperation, conducted in coordination with the Brazilian Cooperation Agency (ABC/MRE), contributes to disseminating a data governance model adapted to the realities of developing countries, balancing the protection of fundamental rights with the challenges of digital-economy growth.

Data Processing and Information Technology Company for Social Security (Dataprev)

Brazil has a consistent regulatory framework for international data flows, centered on the LGPD and the regulations of the National Data Protection Authority (ANPD), especially Resolution No. 19/2024.

Among the mechanisms adopted are:

- Adequacy decisions;
- Standard contractual clauses;
- Technical and legal safeguards;
- Risk assessment and compliance mechanisms.

The mutual recognition of adequacy between Brazil and the European Union (2026) represents a significant advance, promoting secure flows and favoring economic and technological relations.

In addition, international initiatives, such as data intermediaries and trusted sharing arrangements, expand access to data for innovation, research, and public policy, while maintaining high governance standards.

National Data Protection Authority (ANPD)

To date, the main partnership fostering equitable and interoperable data governance in which Brazil participates is the Brazil-European Union Adequacy Decision, signed in January 2026. Broadly, the Decision corresponds to mutual recognition, by Brazil and the European Union (EU), that the protection afforded to personal data by their respective laws is equivalent, allowing such information to circulate between the parties directly, securely, and in a simplified manner, without the need for additional transfer mechanisms. It is, therefore, a mechanism that promotes legal interoperability between Brazil and the EU regarding data protection.

Although recently in force, which makes it difficult to gauge impacts numerically, this partnership has the potential to bring numerous benefits to Brazilian society. At the individual level, the initiative guarantees Brazilian citizens that their personal data will receive the same level of protection afforded to Europeans when transferred or shared with EU countries, with strict rules, effective oversight, and remedy mechanisms in case of misuse. For the business sector, the adequacy decision reduces bureaucracy and costs, since sending data

between Brazil and EU countries no longer requires other international data-transfer mechanisms. As a result, there is increased competitiveness, easier digital business, and expanded access to the European market, which encompasses approximately 450 million consumers. It is estimated that, as a result of this partnership, digital trade could grow by 7% to 9%.

Furthermore, from an economic and innovation perspective, the adequacy decision is expected to foster cooperation in areas such as scientific research, health, artificial intelligence, data science, and emerging technologies, facilitating joint projects among universities, research centers, government bodies, and companies. This reinforces Brazil's attractiveness for investment, innovation, and global partnerships backed by legal certainty and clear rules. Additionally, with the signing of the partnership, the world's largest area of secure data flow is established, encompassing about 700 million people, and Brazil reinforces its institutional maturity while gaining greater international trust.

It should also be noted that establishing this type of partnership demands a high level of engagement and resources. Given its scope, allowing the free flow of personal data, the adequacy decision referred to here was the subject of intense negotiations, involving years of diplomatic and legal effort. In this context, the challenge of promoting a convergence of legislation that balances the free flow of data with the protection of data subjects' rights in foreign territories stands out.

Beyond the adequacy decision with the EU, at the bilateral level, Brazil, through the ANPD, also signs Memoranda of Understanding with data protection authorities of other countries. Generally, these instruments aim to promote institutional collaboration between the ANPD and foreign authorities to strengthen data protection, privacy, and digital governance. Their focus is on the exchange of experiences and regulatory good practices, as well as capacity-building and institutional development. In this sense, such memoranda contribute to more equitable data governance, insofar as they foster the exchange of knowledge and information and promote alignment among data protection authorities.

Currently, 8 (eight) Memoranda of Understanding between the ANPD and other foreign data protection authorities are in force, namely: with the Spanish Data Protection Agency (AEPD); with the Office of the Privacy Commissioner (OPC) of Canada; with the Personal Data Protection Service (PDPS) of Georgia; with the Data Protection Agency (APD) of Angola; with the Public Information Access Agency (AAIP) of Argentina; with the Information Commissioner's Office (ICO) of the United Kingdom and Northern Ireland; with the Catalan Data Protection Authority (APDCCAT) of the Kingdom of Spain; and, finally, with the Dubai International Financial Centre Authority (DIFC), of the United Arab Emirates.

Although these are non-binding mechanisms with a much lower level of institutionalization than an adequacy decision, these memoranda are important for establishing a common basis of understanding among the data protection authorities involved, promoting their institutional strengthening. Furthermore, they may pave the way for more institutionalized cooperation initiatives — including legal and/or technical interoperability — such as an adequacy decision itself.

At the multilateral level, Brazil has been notable for its participation in regional and global networks and forums, which, similarly to Memoranda of Understanding, seek to encourage dialogue and knowledge exchange. In addition to contributing to the promotion of more equitable digital governance by facilitating the democratization of knowledge, these forums and networks can also promote a certain degree of legal interoperability through the adoption of common models and standards.

In this context, one example that stands out is the Ibero-American Data Protection Network (RIPD), in which Brazil has participated since 2021. The Network's central objective is to foster, maintain, and strengthen a close and permanent exchange of information, experiences, and knowledge, as well as to promote the regulatory developments needed to ensure advanced regulation of the right to personal data protection in a democratic context. Among RIPD's initiatives, its model contractual clauses stand out — standardized instruments to ensure the secure international transfer of personal data. By providing a standardized model, they facilitate cross-

border data flows, thereby promoting regulatory convergence and a mechanism of legal interoperability among adopting countries.

More recently, largely inspired by RIPD itself, the Lusophone Data Protection Network (RLPD) was created — with intense Brazilian participation. Like the RIPD, the RLPD serves as a space for cooperation, dialogue, and information-sharing for the development of data protection and privacy initiatives and policies; however, due to its recent establishment, its efforts toward more interoperable governance are still quite incipient.

In addition, among the networks, the Inter-American Network for Digital Government (GEALC) deserves mention. Although it does not specifically address data protection, the GEALC Network makes important contributions to interoperable data governance, insofar as it seeks to facilitate cross-border digital service delivery without barriers in the Latin America and Caribbean region. In this sense, two important initiatives developed within the Network stand out: the first is the Program for Strengthening Cross-Border Electronic Transactions in Latin America and the Caribbean, whose objective is to build capacity and support the implementation of cross-border electronic signatures and cross-border digital services. The national agendas of the countries involved recognize that electronic signatures, like digital identity, are a key point for secure electronic transactions, with potential impact on trade, health, education, and human mobility. The second notable initiative developed within GEALC is IdLAC, a system developed with support from the Inter-American Development Bank (IDB) that connects national digital identities. With this, a citizen of one country can use their own authentication account to access services in another country within the Network. By promoting technical interoperability, these projects also require alignment at the legal level for data sharing, thus fostering coordinated governance at the regional level.

Beyond networks, international forums also serve as spaces for dialogue and joint construction. One of the largest forums in which Brazil participates is the Global Privacy Assembly (GPA), which brings together more than 140 data protection authorities. Within the GPA, interoperability is a central topic of discussion, focusing on the harmonization of legislation, facilitating international transfers, and promoting the recognition of legal equivalences among different countries. As an example of action taken by the forum, one can cite a mapping and comparison study of various standard contractual clauses, carried out by the Working Group on Global Frameworks and Standards, aimed at identifying points of convergence so that different jurisdictions recognize equivalent transfer mechanisms. In addition, a resolution on Data Free Flow with Trust (DFFT) was also approved within the GPA, a framework that seeks to promote secure cross-border transfers of personal data among countries without compromising privacy protection. The resolution reinforces the importance of privacy and data subjects' rights while encouraging regulators to promote convergence and interoperability among different legal tools and reiterates the need for companies to demonstrate accountability in data processing.

Finally, mention should also be made of the partnership between Brazil and the Organisation for Economic Co-operation and Development (OECD). Generally, this partnership is built through a process of regulatory convergence and public-policy assessment, including adherence to the OECD Council Recommendation on Privacy and Transborder Flows of Personal Data. Understanding the importance of data flows for trade and the international economy, this Recommendation aims at harmonizing data protection legislation, fostering interoperability among different regulatory frameworks, and encouraging a free, secure, and reliable data flow.

Ministry of Health (MS)

Brazil participates in various regional and international initiatives aimed at strengthening health data governance, notably actions developed within Mercosur related to digital health and epidemiological surveillance, and cooperation with multilateral bodies such as the World Health Organization (WHO) and the Pan American Health Organization (PAHO), on topics such as standardization, interoperability, and health data sharing. Experience shows that these cooperation mechanisms contribute to sharing good practices, strengthening interoperable standards, data qualification, and the exchange of knowledge and experiences among countries and institutions.

27. In addition to these initiatives, Brazil actively participates in international networks focused on digital transformation and health data governance. Notable is the Global Digital Health Partnership (GDHP), the largest

intergovernmental digital health platform supported by the WHO, which brings together national authorities to develop and share good practices in areas such as interoperability, data governance, cybersecurity, regulatory environments, and digital-policy evaluation. Brazilian participation in these forums contributes to alignment with international standards, the exchange of experiences among countries, and the strengthening of national governance and interoperability capacities.

28. Regionally, Brazil also participates in the activities of the Pan-American Highway for Digital Health (PH4H), an initiative led by the Inter-American Development Bank (IDB), PAHO, and Latin American and Caribbean countries to promote interoperability and secure health-information exchange among countries. Through PH4H's Connectathons and working groups, countries test standards and solutions for cross-border data sharing, including the International Patient Summary (IPS) and digital vaccination certificates, strengthening continuity of care, regional technical cooperation, and the construction of a common interoperability architecture.
29. In the field of bilateral cooperation, notable is the Strategic Sector Cooperation (CSE) between Brazil and Denmark, which has promoted the exchange of experiences on health digitalization, data governance and use, interoperability, and the development of health information infrastructures. The partnership has contributed to strengthening institutional capacities and sharing experiences related to the use of data for management, research, and evidence-based public policy formulation.
30. Brazil also participates in discussions held within BRICS on digital health, artificial intelligence, and health data governance. These initiatives have emphasized the importance of interoperability, data protection, digital sovereignty, institutional capacity-building, and the exchange of experiences among member countries, recognizing data governance as a fundamental element for the resilience of health systems and the development of secure, ethical, and public-interest-oriented digital solutions.
31. Among the main challenges are coordination among different national legislations, including personal-data-protection requirements such as the LGPD and equivalent regulatory frameworks in other countries; building trust for information sharing; semantic interoperability at the international level; and inequalities in institutional capacity among the various participants. These challenges highlight the importance of cooperation mechanisms capable of promoting secure, responsible, and efficient data sharing, respecting national legal frameworks and contributing to strengthening institutional capacities and data governance at the regional and global scale.

7) How can international cooperation strengthen equitable and interoperable data governance to ensure that data contributes to shared prosperity and sustainable development? In what ways can the UN CSTD contribute to this effort?

Ministry of Science, Technology and Innovation (MCTI)

International cooperation is essential for the development of common technical standards, the promotion of interoperability, and the establishment of legal frameworks capable of reducing power asymmetries between States and large global corporations. In this context, the United Nations Commission on Science and Technology for Development (CSTD) plays a relevant role as the United Nations' principal intergovernmental forum for discussions on the impacts of science, technology, and innovation on development. Furthermore, through the exchange of analytical and regulatory frameworks related to the digital economy and data flows, the Commission can contribute to reducing technological dependencies and promoting more equitable data governance.

Ministry of Development, Industry, Trade and Services (MDIC)

Within the framework of the National Data Economy Policy, supporting actions related to data spaces. It is worth highlighting European pioneering and wide dissemination of spaces dedicated to data sharing (data spaces). Data spaces are a technological solution consisting of a federated data system in which different participants share data securely, sovereignly, and with structured governance, retaining control over their strategic assets and data. Data spaces have been widely disseminated in Europe and are recognized as a pioneering and fundamental technological solution for organizing data in the digital economy, ensuring both

technical and regulatory security by design. These characteristics provided by this technological solution have proven fundamental to encouraging the use and sharing of data. In this sense, these data spaces have been widely adopted to enable data exchange by the productive sector and governments, in various experiences around the world, including under different names, such as Data Trusts (USA) or Data Exchanges (China).

The UNCTAD CSTD can contribute by promoting data-space pilot projects with Brazilian and international participation; supporting the development of secure and interoperable digital infrastructure; and encouraging the integration of industrial data, traceability, and supply chains to simultaneously boost competitiveness, innovation, and economic development.

Ministry of Justice and Public Security (MJSP) — Information and Communication Technology Sub-Secretariat

International cooperation can strengthen equitable and interoperable data governance through technical incentives such as: sharing existing guidelines, technical studies, and best-practice forums; offering training courses for public servants; and fostering ongoing projects with financial resources and technical support capable of accelerating the implementation of data governance initiatives and outcomes focused on equitable and interoperable data governance to ensure that data contributes to shared prosperity and sustainable development.

The CSTD can lead support and monitoring working groups for existing and new data governance initiatives within Public Administration bodies, promote forums and workshops aimed at addressing concrete challenges, exchanging knowledge, and encouraging innovation.

Ministry of Justice and Public Security (MJSP) — National Secretariat for Digital Rights, Data Protection Coordination-General

Brazil believes international cooperation is key to building a global digital economy that benefits everyone. The country advocates for data governance that promotes shared prosperity, recognizing the fundamental role of developing countries in the global data value chain.

UNCTAD data indicate that more than 80 countries have adopted data protection legislation, but the effectiveness of these rules is highly uneven, reflecting disparities in regulatory capacity, technological infrastructure, and negotiating power in international forums.

Brazil proposes that international cooperation advance on the following strategic fronts:

- **Capacity-building:** Promoting partnerships for knowledge exchange and technical support for consolidating data protection authorities worldwide;
- **Inclusive transfer mechanisms:** Developing multilateral frameworks that facilitate data flows, recognizing the diversity of regulatory approaches and ensuring rights protection;
- **Sustainable development:** Fostering business models and cooperation arrangements that encourage investment in digital infrastructure and innovation in developing countries;
- **Interoperability:** Promoting dialogue for the harmonization of principles and standards, respecting each nation's sovereign characteristics and choices;
- **Participatory governance:** Strengthening multilateral forums that ensure representativeness of all countries and sectors of society in formulating global guidelines.

UNCTAD's Commission on Science and Technology for Development plays a unique and indispensable role in this scenario. Its development vocation and universal legitimacy make it the ideal forum to lead the construction of more equitable data governance.

Brazil suggests the CSTD consider the following initiatives:

- Promoting guiding principles on data governance for development, serving as a reference for good practices;

- Fostering research and monitoring of global digital-economy dynamics, supporting evidence-based public policymaking;
- Supporting the creation of spaces for dialogue and cooperation among data protection authorities from different regions;
- Encouraging technical capacity-building programs on data governance and artificial intelligence;
- Promoting debates on the intersection of data protection, digital rights, and international trade.

Data Processing and Information Technology Company for Social Security (Dataprev)

Despite progress, significant challenges remain, such as international regulatory fragmentation, institutional-capacity inequalities, and compliance costs, especially in developing countries.

International cooperation is fundamental for:

- Promoting common interoperability standards;
- Regulatory harmonization;
- Strengthening institutional capacities;
- Reducing integration costs;
- Expanding access to digital infrastructure.

In this context, the Commission on Science and Technology for Development (CSTD) can play a strategic role by:

- Fostering the exchange of good practices;
- Supporting the development of technical and institutional capacities;
- Promoting global data-governance frameworks;
- Encouraging models that reconcile data protection, interoperability, and sustainable development.

National Data Protection Authority (ANPD)

Given the essentially transnational nature of data, it is natural that international cooperation efforts represent a fundamental pillar of data governance and protection. In this sense, international cooperation can strengthen equitable and interoperable data governance through different fronts, including the standardization of norms and formats and regulatory harmonization, the strengthening of technical and institutional capacities, the advancement of digital public infrastructure, and the promotion of an equitable distribution of benefits.

In terms of technical interoperability, international cooperation plays a relevant role in promoting the standardization of norms, formats, and protocols. More technically-oriented initiatives can foster the sharing of metadata standards and the dissemination of open-source models and open APIs, allowing datasets to communicate seamlessly across borders. IdLAC, developed within the GEALC Network and referenced in question 6, is an example of this type of collaboration. Furthermore, international cooperation can also foster the creation of federated data models, in which different countries can have a unified view of information from distinct sources, for example, through tiered access agreements.

Although technical interoperability is an important part of data sharing, it alone is not always able to guarantee the security of such data; hence the need for legal interoperability as well. By promoting dialogue and the exchange of experiences and good practices, initiatives such as Memoranda of Understanding (MoUs) and participation in networks and forums can contribute to regulatory alignment and legal interoperability. In this context, closer relations between governments and among data protection authorities enable convergence of jurisdictions and foster mutual trust that transferred and/or shared data will receive due protection. More robust cooperation efforts, such as adequacy decisions, enable countries to enjoy the benefits of data access without compromising its security.

Beyond promoting legal interoperability, participation in multilateral blocs and bodies helps strengthen countries' technical and institutional capacities. The exchange of knowledge and good practices promoted within these spaces democratizes access to information, allowing countries with incipient data regulations to

learn from the experience of others, and accelerates the institutional consolidation of data protection authorities. This advances more horizontal and equitable data governance at the international level.

International cooperation can also strengthen more interoperable and equitable data governance by advancing digital public infrastructure. Broadly, digital public infrastructure corresponds to an ecosystem of interoperable, secure systems serving the public interest, such that its development has a direct impact on service delivery to citizens. Cooperation initiatives, in this sense, can include collaborative investments in open-source software and/or open datasets, as well as the promotion of guidelines for establishing internationally interoperable, secure, user-centered infrastructures — such as those advocated by the United Nations Global Digital Compact. This makes available, including to developing countries, the basic tools to provide essential services to society, in areas such as health and finance.

Last but not least, cooperation efforts, whether bilateral or multilateral, can help developing countries gain access to the physical and technological infrastructure needed to better harness the value of data. Investments in technology infrastructure, technical cooperation agreements, and knowledge exchange allow these countries to develop their own data capacities, from data centers to national AI models, moving beyond the mere export of raw data toward retaining local computing capabilities. This shift is essential for less-developed nations to maximize the benefits they extract from their data across the entire value chain, thereby enabling greater distributive equality and more equitable governance on a global scale.

It is thus clear that international cooperation is not only a fundamental instrument but also offers a range of fronts — the ones mentioned above being non-exhaustive — through which it can contribute to equitable and interoperable data governance. Deeply interrelated, these two conditions (equality and interoperability) lie at the heart of promoting shared prosperity and sustainable development.

To overcome historical power imbalances, equitable data governance requires policies, algorithms, and practices that prioritize transparency and inclusive participation over narrow profit maximization. This means treating data as a collective good — not a commodity — redistributing private gains to the public domain and ensuring they contribute to the common good and national development objectives. It is, therefore, about ensuring that the benefits of data capacities and the insights extracted from them fairly serve all communities. For this, however, it is imperative that access to such data be democratic.

In this sense, interoperability emerges as a way of technically enabling data access while simultaneously providing legal certainty to this process. The importance of allowing data to be accessed and shared, in turn, derives from the economic and social impact such data can generate. According to an OECD report, studies indicate that data access and sharing can contribute to generating benefits of up to 1.5% of Gross Domestic Product (GDP) in the case of public-sector data, and up to 2.5% of GDP when private-sector data is also involved. In this context, by expanding the reach of data, technical and legal interoperability can provide (i) greater transparency and accountability; (ii) new business opportunities; (iii) competition and cooperation within and among different sectors and countries; (iv) crowdsourcing and user-driven innovation; and (v) greater efficiency in service delivery, due to data integration.

Thus, maintaining interoperability is necessary for datasets and data regimes to be compatible with one another and to maximize the benefits of data sharing, while equitable governance seeks to ensure that such benefits are distributed fairly and for the collective good. They are, therefore, two gears of the same system that move together to allow data to serve everyone (shared prosperity) and for the benefits extracted from it to generate ethical, fair growth aimed at reducing inequalities and guaranteeing rights (sustainable development).

Given this, it is understood that the United Nations CSTD can contribute to equitable governance and interoperability through multifaceted action that promotes cooperation across different fields, spanning the promotion of standardized norms and formats, regulatory alignment, the strengthening of technical and institutional capacities, the advancement of digital public infrastructure, and the encouragement of a fair distribution of benefits. In this regard, the organization's role in promoting dialogue among different actors stands out, as demonstrated by the Working Group on Data Governance at All Levels, by providing a space for

governments, the private sector, and civil society to discuss how to ensure that the benefits of innovation are shared. Furthermore, it is essential that the data-governance guidelines and principles advanced by the CSTD bear in mind the protection of fundamental rights and the achievement of the Sustainable Development Goals (SDGs). Therefore, as the world's largest intergovernmental body, it is important that the United Nations continue fostering relevant debates on data governance, promoting different vectors of cooperation, while allowing member states to exercise their sovereignty in the digital environment.

Ministry of Health (MS)

International cooperation plays a fundamental role in strengthening equitable, interoperable, and sustainable-development-oriented data governance. Interoperability among systems depends on the existence of common technical standards, clearly defined governance mechanisms, and reliable information-sharing processes. In this context, international cooperation can contribute to disseminating good practices related to digital identification, interoperability, data quality, and information governance, favoring the construction of more integrated, reliable, and inclusive data ecosystems.

33. The United Nations Commission on Science and Technology for Development (CSTD) can support this process by promoting the exchange of experiences among countries, identifying and disseminating successful data-governance models, developing open global interoperability standards, and strengthening technical training and data-governance programs. At the same time, it is important that such efforts be coordinated with existing initiatives at the regional and international levels, in order to avoid fragmentation of initiatives, overlapping agendas, and duplication of efforts and resources, promoting greater convergence and complementarity among different cooperation forums and mechanisms.
34. It should also be emphasized that international cooperation can help support the development of digital infrastructure in developing countries, promote the transfer of knowledge and good practices, and foster mechanisms for the fair distribution of benefits derived from data use. Brazil recognizes that such efforts are essential to expand institutional capacities, strengthen trust in information sharing, and ensure that data contributes to shared prosperity, digital inclusion, and sustainable development.

Final Considerations

Ministry of Development, Industry, Trade and Services (MDIC)

Brazilian experience in building a robust personal data protection framework, from the passage of the LGPD to the consolidation of the National Data Protection Authority as an independent agency, offers relevant lessons for the international debate on data governance for development.

The Brazilian government understands that data governance is a strategic pillar for sustainable development and the country's competitive positioning in the global economy. Brazil advocates for an international digital order based on cooperation, trust, and mutual benefit.

The National Secretariat for Digital Rights (SEDIGI) reaffirms its willingness to actively collaborate with other CSTD member states and the UNCTAD Secretariat, contributing Brazilian experience to advancing this important global agenda.

It should be noted that this contribution reflects the perspective of the Data Protection Coordination-General. The Brazilian government will continue working in an integrated manner to provide comprehensive, multisectoral input to the Commission's debates.

Data Processing and Information Technology Company for Social Security (Dataprev)

The evolution of data governance in Brazil highlights the importance of adopting structured approaches that integrate technical, regulatory, and institutional dimensions.

The consolidation of an interoperable, secure, value-oriented data ecosystem requires continuous investment in digital infrastructure, open standards, data management, information security, and capacity-building.

The promotion of equitable and interoperable data governance is an essential condition for maximizing the economic and social benefits of data, contributing to sustainable development and the modernization of the State.

References

- 1 ^ https://www.cgi.br/media/docs/publicacoes/6/pt-br/20251209175312/psi-a17-n4-data_centers_no_brasil.pdf
- 2 ^ <https://www.datacentermap.com/brazil/>
- 3 ^ <https://www.datacentermap.com/western-europe/>
- 4 ^ <https://www.datacentermap.com/usa/>
- 5 ^ <https://www2.camara.leg.br/legin/fed/medpro/2025/medidaprovisoria-1318-17-setembro-2025-797988-exposicaodemotivos-176542-pe.html>
- 6 ^ <https://cetic.br/pt/tics/domicilios/2025/domicilios/>
- 7 ^ <https://www.anatel.gov.br/paineis/aceessos>
- 8 ^ <https://ix.br/localidades/atuais>
- 9 ^ <https://cetic.br/pt/tics/domicilios/2025/domicilios/>
- 10 ^ https://blogs.worldbank.org/en/voices/digital-inclusion-unlocks-more-resilient-recovery_-all
- 11 ^ <https://brasscom.org.br/wp-content/uploads/2025/08/Estudo-sobre-o-Consumo-de-Energia-e-Agua-em-Data-Centers-no-Brasil-v7.pdf>
- 12 ^ <https://www.gov.br/fazenda/pt-br/central-de-conteudo/publicacoes/apresentacoes/2025/Maio/pndc-audiencia-publica-pl3018-maio25.pdf>

- 8 [^] <https://jornal.usp.br/campus-ribeirao-preto/expansao-dos-data-centers-no-brasil-pode-por-em-risco-a-transicao-energetica/>
- 14 [^] <https://www.gov.br/fazenda/pt-br/central-de-conteudo/publicacoes/apresentacoes/2025/Maio/pndc-audiencia-publica-pl3018-maio25.pdf>
- 16 [^] <https://fesauesp.org.br/ultimas-noticias/o-que-falta-para-a-interoperabilidade-deixar-de-ser-excecao-no-brasil/>
- 16 [^] https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/11/enhancing-access-to-and-sharing-of-data_070835df/276aaca8-en.pdf
- 17 [^] https://unctad.org/system/files/official-document/der2021_en.pdf
- 18 [^] <https://www.cgi.br/media/docs/publicacoes/6/pt-br/20251209175312/psi-a17-n4-data-centers-no-brasil.pdf>
- 19 [^] <https://jornal.usp.br/campus-ribeirao-preto/expansao-dos-data-centers-no-brasil-pode-por-em-risco-a-transicao-energetica/>
- 20 [^] <https://www.gov.br/anpd/pt-br/assuntos/noticias/brasil-e-uniao-europeia-reconhecem-adequacao-mutua-em-protecao-de-dados-pessoais>
- 21 [^] <https://www.gov.br/planalto/pt-br/acompanhe-o-planalto/noticias/2026/01/alckmin-celebra-reconhecimento-mutuo-para-transferencia-de-dados-entre-brasil-e-uniao-europeia-201cinvestimentos-reciprosos201d>
- 22 [^] <https://www.gov.br/anpd/pt-br/assuntos/noticias/brasil-e-uniao-europeia-reconhecem-adequacao-mutua-em-protecao-de-dados-pessoais>
- 23 [^] <https://www.gov.br/anpd/pt-br/aceso-a-informacao/convenios-e-transferencias/repases-e-transferencias-de-recursos-financeiros/1-termo-aditivo-memorando-de-entendimento-anpd-aepd-em-portugues.pdf/@@display-file/file>
- 24 [^] https://www.gov.br/anpd/pt-br/aceso-a-informacao/convenios-e-transferencias/documentos/mde_anpd-opc_pt_ocultado.pdf/@@display-file/file
- 25 [^] <https://www.gov.br/anpd/pt-br/aceso-a-informacao/convenios-e-transferencias/repases-e-transferencias-de-recursos-financeiros/memorando-de-entendimento-anpd-pdps-em-portugues.pdf/@@display-file/file>
- 26 [^] <https://www.gov.br/anpd/pt-br/aceso-a-informacao/convenios-e-transferencias/repases-e-transferencias-de-recursos-financeiros/memorando-de-entendimento-anpd-apd-em-portugues.pdf/@@display-file/file>
- 27 [^] <https://www.gov.br/anpd/pt-br/aceso-a-informacao/convenios-e-transferencias/repases-e-transferencias-de-recursos-financeiros/memorando-de-entendimento-anpd-aap-em-portugues.pdf/@@display-file/file>
- 28 [^] <https://www.gov.br/anpd/pt-br/aceso-a-informacao/convenios-e-transferencias/repases-e-transferencias-de-recursos-financeiros/memorando-de-entendimento-anpd-ico-em-portugues.pdf/@@display-file/file>
- 29 [^] <https://www.gov.br/anpd/pt-br/aceso-a-informacao/convenios-e-transferencias/repases-e-transferencias-de-recursos-financeiros/memorando-de-entendimento-anpd-apdcat-em-portugues.pdf/@@display-file/file>
- 30 [^] <https://www.gov.br/anpd/pt-br/aceso-a-informacao/convenios-e-transferencias/repases-e-transferencias-de-recursos-financeiros/memorando-de-entendimento-anpd-difc-em-portugues.pdf/@@display-file/file>
- 31 [^] <https://globalprivacyassembly.com/wp-content/uploads/2025/10/GFSWG-Annual-Report-2025.pdf>
- 32 [^] <https://globalprivacyassembly.com/wp-content/uploads/2024/11/Resolution-Data-Free-Flow-with-Trust-and-an-effective-regulation-of-global-data-flows.pdf>
- 33 [^] <https://www.un.org/global-digital-compact/en>
- 34 [^] https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/11/enhancing-access-to-and-sharing-of-data_070835df/276aaca8-en.pdf

