United Nations Development Programme

Data Governance Framework

Recommendation Report for Türkiye

UNDP is the leading United Nations organization fighting to end the injustice of poverty, inequality, and climate change. Working with our broad network of experts and partners in 170 countries, we help nations to build integrated, lasting solutions for people and planet.

Learn more at undp.org or follow at @UNDP.

This report was prepared by the United Nations Development Programme (UNDP) Türkiye Country Office and Chief Digital Office (CDO) in collaboration with the Digital Transformation Office of the Presidency of the Republic of Türkiye (DTO).

Photo credits: Images used from shutterstock.com and stock.adobe.com.

Table of Contents

Acronyms

AI	Artificial Intelligence
APEX	API Exchange
APIs	Application Programming Interfaces
ASEAN	Association of Southeast Asian Nations
CBRT	Central Bank of the Republic of Türkiye
CDO	Chief Digital Office
CSOs	Civil Society Organizations
DCAT-AP	Data Catalogue Application Profile
DPGs	Digital Public Goods
DPI	Digital Public Infrastructure
DPIA	Data Protection Impact Assessment
DTO	Digital Transformation Office of the Presidency of the Republic of Türkiye
EU	European Union
EVAM	Electronic Data Research Center
FAIR	Findability, Accessibility, Interoperability and Reusability
GBS	Entrepreneur Information System
GIS	Geographical Information System
GDPR	General Data Protection Regulation
HR	Human Resources
IDS	International Data Spaces
KVKK	Personal Data Protection Law (No. 6698)
MAKS	Spatial Address Registration System
NAIS	National Artificial Intelligence Strategy
NSS	National Statistical System
OECD	Organisation for Economic Co-operation and Development
OHCHR	Office of the High Commissioner for Human Rights
OOP	Once-only principle
OSP	Official Statistics Programme
PPPs	Public-Private Partnerships
SDGs	Sustainable Development Goals
TÜBİTAK	Scientific and Technological Research Council of Türkiye
TUCBS	Turkish National Geographic Information System
TurkStat	Turkish Statistical Institute
TSS	Turkish Statistical System
UK	United Kingdom
ULAKBİM	Turkish Academic Network and Information Center
UN DESA	United Nations Department of Economic and Social Affairs
UNDP	United Nations Development Programme
USA	United States of America
VERBIS	Data Controllers Registry Information System

Executive summary

Establishing a robust data governance framework can help build a future where data serves people. Such a framework can enable efficient, secure and rights-based data exchanges, both domestically and across borders, while mitigating the risks related to data such as data breaches, security, compliance violations and data quality problems. It can ensure data privacy is protected within and across organizations, and it can promote the responsible and ethical use of data for the delivery of public services and the advancement of policy initiatives.

In Türkiye data plays an increasingly important role in development – not least because more and more data has been generated across many different sectors of government. Yet, data is not always accessible to the relevant stakeholders and different datasets are often not aligned. Challenges span multiple data types including: administrative data, operational data, transactional data, big data and open data. A robust data governance framework is a vital element of addressing those challenges. By defining parameters for data access, use, reuse and sharing the framework can act as a catalyst for Türkiye's digital transformation.

This becomes ever more important as the evolving nature of Türkiye's requirements increases the need to prevent data from becoming siloed. Clear rules and regulations governing data sharing and technical data standards are also necessary. Open data shows huge potential but currently lacks guiding laws and platforms for access. And the paradigm shift required for the new digital transformation in Türkiye is dependent on clear and solid big data governance to enable the responsible use of Artificial Intelligence (AI) and analytics.

Türkiye has expended great efforts on data governance in recent years, especially after the Turkish Statistical Law[1] was published in 2005 under the leadership and coordination of the Turkish Statistical Institute (TurkStat). In 2016, Personal Data Protection Law No. 6698 (KVKK) was passed: the first law that regulates the protection of personal data. The Personal Data Protection Authority, a public legal entity with administrative and financial autonomy, was established under this law. The National Data Dictionary Project, a project of the Digital Transformation Office of the Presidency of the Republic of Türkiye (DTO), also plays an important role by working to create a common language between information systems. The Ministry of Environment, Urbanization and Climate Change is implementing the Turkish National Geographic Information System (TUCBS) project. This will create a portal for geographic data which will enable public institutions and organizations to share information. There are many more similar examples.

Although there is no comprehensive national data governance strategy in Türkiye, its importance has been noted in relevant policy and strategy documents and several measures have already been taken. The responsibility for establishing a Data Governance Working Group and supporting its initiatives was assigned to the DTO in the 2022 Annual Presidential Program, published by the Presidency of Strategy and Budget. The 2024 Annual Presidential Program[2], issued in October 2023, also includes the preparation of a national data strategy by the DTO as one of its measures.

In this context, United Nations Development Programme (UNDP) is implementing a project which aims to support Türkiye in data governance by providing its expertise in the form of key policy recommendations. In collaboration with the DTO, UNDP's Türkiye Country Office and Chief Digital Office (CDO) initiated efforts to research and outline recommendations towards designing a data governance framework.

[1] Türkiye, Turkish Statistical Law, 2005, https://www.tuik.gov.tr/Kurumsal/Turkiye_Istatistik_Kanunu
[2] Türkiye, the Presidency of Strategy and Budget, 2024 Annual Presidential Program (2023), https://www.sbb.gov.tr/wp-content/uploads/2023/10/2024-Yili-Cumhurbaskanligi-Yillik-Programi.pdf

This indicative data governance framework is based on a needs assessment conducted through a multi-stakeholder consultation process that included ministries, other government institutions, municipalities, universities, Civil Society Organizations (CSOs) and the private sector, as well as country case studies and a review of the data governance frameworks of international organizations.

UNDP has developed a conceptual framework for Türkiye's data governance covering suggested principles, pillars and mechanisms. It encompasses UNDP's primary recommendations and suggested action points. This report is not designed to serve as an exhaustive set of guidelines, or to provide a manual for data governance, but rather is designed to offer strategic insights and contextual understanding that will provide national stakeholders with helpful guidance.

Data governance in Türkiye should be firmly rooted in ethical principles based on human rights. This must guide the collaborative, responsible, transparent stewardship of data.

The data governance framework can be anchored in the following principles:
- Protect human rights,
- Adopt an inclusive approach,
- Maintain ethical standards,
- Empower people through data,
- Promote accountability,
- Promote transparency,
- Promote a culture of data innovation, learning and sharing.

The recommended data governance framework for Türkiye encompasses the following five pillars:

1. Policies, legislation and regulations,
2. Institutions, mechanisms and processes,
3. People,
4. Technology and infrastructure,
5. Partnerships.

Below is a summary of UNDP's recommendations under each pillar in detail. These are further elaborated in Section D.

Summary recommendations

Pillar 1: Policies, legislation and regulations

To ensure effective data governance and data protection Türkiye should **strengthen its legislative framework for data (Recommendation 1.1)**. Working towards harmonizing Türkiye's data legislation with global and regional regulations would advance the state's national priorities and help it to meet international requirements. This process should involve a meticulous evaluation of the various legal approaches for non-personal data taken by other countries. In particular, given Türkiye's long-term goal of becoming a member of the European Union (EU), it should consider how it can work towards compatibility with the EU Data Governance Act and Data Act.

As most institutions of government have their own unique regulations, an overarching cross-governmental **framework legislation for data governance** is recommended to avoid discrepancies.

A data sharing governance framework commitment document[3] can also be prepared so that stakeholders can declare their commitment to proactively sharing data in simpler and faster ways.

[3] United Kingdom, Central Digital and Data Office, Data Sharing Governance Framework (2022), https://www.gov.uk/government/publications/data-sharing-governance-framework/data-sharing-governance-framework

The second component is **the development of a national data strategy (Recommendation 1.2)** supported by clear and actionable guidelines and standards. **Practical action plans** for public sector institutions can build on top of this to identify and prioritize data management activities in a given year. This will ensure focused, measured progress.

Türkiye should also **ensure that sector-specific regulations align with broader data governance policies (Recommendation 1.3) The impact of sector-specific legislation** (including administrative registers and privately held databases) on other sectors or stakeholders should be **assessed by a multi-stakeholder mechanism** to conduct a "risk-benefit analysis." In addition to this comprehensive assessment, government institutions should develop a **data sharing risk assessment model**[4] for non-personal data. This mitigates the risks of data sharing by considering issues beyond data sensitivity such as: which organisations the data will be shared with, how it will be shared and what it will be used for. This model should be consistent across government bodies, should be flexible enough to adapt to changing demands and priorities and should consider the impact of not sharing data.

The EU Data Governance Act[5] provides a framework to enhance trust in voluntary data sharing for the benefit of businesses and citizens. It can act as a helpful guide in strengthening data legislation in Türkiye. It covers various aspects of data sharing including data re-use (including with respect to protected data held by public sector bodies), data intermediation services (intermediaries who connect data providers with users; they cannot monetize data) and data altruism. Data altruism is defined in the Act as the sharing of data in support of objectives of general interest such as healthcare and combatting climate change.

Data protection policies and regulations for both personal data and non-personal data should be effectively implemented (Recommendation 1.4). These policies should consider human rights (including children rights which merit specific protection with regards to their personal data), commercially sensitive information and sector-specific data issues. Türkiye should amend the KVKK[6] to ensure stricter protection, and to improve compatibility with international rules and standards such as the EU General Data Protection Regulation (GDPR)[7].

A comprehensive legislation assessment is recommended. This should be done via a multi-stakeholder approach and by involving legal advisors and relevant experts. Such a process might demonstrate the necessity of revising the conditions under which personal data is processed, introducing special categories of personal data and considering exchange of personal data across international borders.

Legal uncertainty should be reduced through non-legislative measures such as: risk analysis, organisational policies and physical and technical measures. Another effective non-legislative approach is to incorporate data protection considerations into the design and development of products, services and systems from the outset. Data Protection Impact Assessments (DPIAs) can identify and mitigate potential privacy risks when high risk data processing activities are developed. Where indicated this can trigger additional training and awareness raising activities.

When it comes to international data transfers, Türkiye should amend the KVKK to bring it into alignment with other sectoral legislation, mutual recognition agreements, decisions by international organizations and relevant bilateral agreements. A multistakeholder approach, involving consultation with legal experts, should consider whether the Data Governance Act and EU Regulation (EU)

[4] Ibid.
[5] European Union, Data Governance Act (2022), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868
[6] Türkiye, Personal Data Protection Law (2016), https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law
[7] European Union, General Data Protection Regulation (2016), https://gdpr.eu/tag/gdpr/

2018/1807, which provides a framework for the free flow of non-personal data in the EU,[8] is suitable for Türkiye.

Pillar 2: Institutions, mechanisms and processes

Strengthening central data management and leadership (Recommendation 2.1) is also necessary. Türkiye should assign core roles and responsibilities with respect to data management; in particular the state should identify data governance leaders and stewards to oversee data-related initiatives and ensure adherence to data governance policies. Legislation can specify who holds paramount authority with respect to issues such as interoperability, use, security and confidentiality. One of the most critical steps is to define and appoint the role of Chief Data Officer. This can inspire the establishment of a national data board or similar bodies to drive effective data governance.

There is a need to **efficiently implement institutional mechanisms (Recommendation 2.2)**, and improve metadata management and the cataloguing and indexing of data to reduce duplication and improve data quality. A structure and decision-making process should be established to guide data access, sharing and interoperability. The roles and responsibilities of various stakeholders in the data ecosystem, including data users, data custodians and committees, should be clearly defined. Further, accountability mechanisms to ensure compliance and effective data governance need to be established. Implementing these reforms will require these institutions to have commitment to, and ownership of, the reform process.

Setting up a **dedicated central data management office** as a designated specific body responsible for overseeing the strategic management of data is recommended. This body shall be responsible for framing, managing and periodically reviewing and revising data policy. It could be established as a governing body with the power to create rules for data governance and data quality management. It can also define and share data-management best practices and support public-sector entities to create their own action plans.

Further, it is recommended to **redesign the data management units within ministries and institutions.** Every ministry and government institution's data management unit should be headed by designated Chief Data Officers working closely with the central data management office.

Coordination mechanisms, including **a national data board and inter-agency working groups,** should also be established to facilitate data-driven decision-making. These mechanisms allow stakeholders such as the DTO, TurkStat, Central Bank of the Republic of Türkiye (CBRT), ministries, government institutions, CSOs, academics, private sector institutions and the media to promote the exchange of data and enhance its utilization in decision-making processes.

By engaging government agencies in the "Public Data Space" and creating related units within the government one can create hubs for data-related expertise, research and collaboration. These hubs can then provide consultancy services and support for data-driven initiatives across government.

The establishment of 'Data-labs' for high-priority use cases is another recommendation. This allows the government to focus on rapid, tangible impact during the period before long term reforms start to have noticeable effects.

[8] European Union, Regulation (EU) 2018/1807 of The European Parliament and of The Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (2018), https://eur-lex.europa.eu/legal-content/ EN/TXT/PDF/?uri=CELEX:32018R1807

An open data portal is an important institutional mechanism for promoting data-driven decision making and fostering transparency and accountability. Türkiye can effectively use this platform to allow all stakeholders in the data ecosystem to publish and share their data with the public and with each other.

Developing a communication mechanism or plan (Recommendation 2.3) across the public sector is important. This will promote a shared vision and understanding of the data agenda.

There is also a need to create mechanisms for **monitoring and evaluating (Recommendation 2.4)** the implementation of data governance policies and practices. This may include regular reviews, audits, compliance checks and penalties for non-compliance. It will also ensure the **continuous improvement and adaptation** of national data strategies, so they remain resilient, adaptable and sustainable, particularly with respect to emerging technologies and evolving data governance challenges.

Pillar 3: People

People is one of the crucial components of the proposed data governance framework, and constitutes its third pillar. By focusing on capacity development and training to strengthen data cultures and data literacy, Türkiye can build a solid foundation for its data governance framework to operate upon and can foster a data-driven society where there is public trust in governmental data processing.

Developing and implementing capacity building programmes (Recommendation 3.1) for data governance is essential. These programmes should target government officials, private sector stakeholders and CSOs and academia, aiming to raise awareness of the importance of data governance and encourage adherence to best practices. These activities should take place as part of the national data strategy and be included in the action plans which will be subsequently developed. Additional **guidelines and reference documents** should be prepared to provide individuals with information on data access and processing.

Developing a human resources strategy and policy (Recommendation 3.2) can help mitigate issues caused by turnover in IT staff in government institutions and ensure adequate support for data governance initiatives. This in turn requires the **development of data-related skills and competencies** with respect to areas such as data standards, data management and data analytics. Staff must be trained to focus on creating innovative services and products and ensuring data security and privacy.

Strengthening Türkiye's data culture (Recommendation 3.3) involves creating an environment where data-driven decision-making is encouraged and valued. Efforts should be made to promote a data-driven mindset and cultivate a culture of using data to inform policies, strategies and operations. Türkiye could develop training programs for relevant staff to this end. Other ways to foster this change include identifying, engaging with and investing in potential champions and prioritising use cases that demonstrate the value and potential impact of data-informed decision making. Türkiye can also support informed and sovereign handling of data by citizens of all age groups through various formal and informal educational opportunities.

Developing data literacy (Recommendation 3.4) is an essential aspect of data governance. This refers to the ability of individuals to understand, analyse and interpret data effectively and to handing it with respect for data privacy and security. Data literacy is important for government officials, private sector stakeholders and the general public.

Pillar 4: Technology and Infrastructure

The fourth pillar is Technology and Infrastructure which plays a crucial role in enabling effective data management, data sharing and data security.

Open-source software and ecosystem solutions (Recommendation 4.1) provide unified and secure data exchange between stakeholders in the data ecosystem. Digital Public Goods (DPGs) are collective digital solutions which freely available for all to modify, add to and deploy. For this reason, well-established, well-supported DPGs and other open-source solutions can be used to build Türkiye's data ecosystem.

Efficient implementation of APIs (Recommendation 4.2) enables seamless integration and exchange of data between different systems and platforms.

Data exchange layers (Recommendation 4.3) allow information to be managed and shared easily but securely among a diverse network of users. Institutions in Türkiye can use a secure open-source data exchange layer such as X-Road for data sharing. Türkiye should also develop strategies for secure data storage, giving consideration to data backup, disaster recovery, data retention periods and current and necessary future data standards.

A cloud strategy (Recommendation 4.4) for Türkiye is already in development; this strategy should be implemented to meet the needs of public institutions.

Deploying a range of tools for analytics (Recommendation 4.5) is another key component of this pillar. These tools can include data integration platforms, data quality management systems, data visualization tools and self-service applications. Empowering users by giving them diverse toolsets enables efficient data analysis, reporting and decision-making.

The improvement of data standards (Recommendation 4.6) includes standardizing data formats, schemas and classifications to facilitate data integration, exchange, and analysis. Registration systems are based on administrative records and effective usage of these records is made possible by international classifications. TurkStat already supports all relevant organizations and users through the Classification Server[9] to enhance the quality of statistics. It is therefore critical to ensure the usage of common classifications by all stakeholders so that data is comparable and reliable. All stakeholders should continue working together to prepare an action plan to come into full compliance with these classifications. **Clearly defining units of measurement and clearly defining variables and their attributes within the data architecture** helps ensure consistency and accurate data representation. Implementing data validation and verification mechanisms can help identify and rectify data inconsistencies.

Establishing a comprehensive metadata system (Recommendation 4.7) which is in line with fundamental data privacy principles (such as data minimization, storage limitation, integrity and confidentiality) is crucial for documenting and managing data-related information. It can also improve data discoverability, understandability, usability and interoperability. DTO and TurkStat can provide guidance on a metadata management model for the data ecosystem. Developing data catalogues provides comprehensive information about available datasets, their characteristics and access mechanisms. Developing these catalogues requires developing guidelines for, and evaluating the quality of, Open Data in Türkiye. AI and machine learning can be used to automate the process of collecting and interpreting the metadata in data catalogues to reduce manual effort.

[9] Türkiye, Turkish Statistical Institute Classification Server (2020), https://biruni.tuik.gov.tr/DIESS/ChangeLocaleAction.do?dil=en

Pillar 5: Partnership

Partnership is the fifth pillar of the framework. Collaboration and partnerships are essential for effective data governance and utilization and can help unlock the full value of data in the public sector.

By **establishing new data sharing arrangements (Recommendation 5.1)** which foster collaboration with the private sector and academia, integrate with other data ecosystems and align with international standards, Türkiye can build strong partnerships that promote data-driven innovation, problem-solving and cooperation at the national and international levels. Signing protocols and agreements with actors in the digital ecosystem solidifies data partnerships, including Public-Private Partnerships (PPPs).

To improve **cooperation and collaboration among stakeholders (Recommendation 5.2)**, government entities can **partner with CSOs, academia and private entities to access data** and accelerate analysis, problem-solving and innovation. Türkiye should actively engage these sectors in the data governance framework using mechanisms such as data research partnerships, data innovation hubs and public-private-academia coordination.

To unlock more value from data, Türkiye should prioritize **further integration with other data ecosystems (Recommendation 5.3).** This means actively seeking partnerships and collaborations with external data sources such as international organizations, research institutions and industry associations. To facilitate cross-border data flows and ensure compatibility with global data governance norms, Türkiye should align its data governance framework with international standards and the frameworks used by partner countries and international institutions.

A. Introduction

1. Background and justification

In todays' world, a well-established digital public infrastructure is crucial to protect citizens' rights, enable the development of data-driven public and private services and ensure inclusion. Fully utilising this potential requires certain foundational elements to be in place. These include an effective digital ecosystem, the presence of appropriate digital infrastructure, the adoption of inclusive multi-stakeholder approaches and the presence of incentives to identify and engage in cross-organizational and cross-border data flows. Given the critical value of digital public infrastructure in enabling governments to operate efficiently, and in managing opportunities and risks, it has become imperative to have strong data governance programmes and frameworks that enable the effective and responsible use of data.

UNDP is the UN's global development network, advocating for change and connecting countries to knowledge, experience and resources to help people build a better life. With a local presence in 170 countries and Accelerator Labs in 91 locations that support 115 countries, UNDP has deep insights into local data governance challenges as well as the capacity to implement initiatives in all parts of the world. UNDP advocates for a data governance framework that safeguards citizens' safety through a people-centred, human rights-based approach that considers data availability, quality, openness and accountability.

Data has the potential to transform industries, to better inform policymaking and ultimately to improve lives. For example, more timely and precise weather data can significantly improve agricultural outputs and improve farming practices. Poverty data can help to better inform poverty reduction strategies and ensure the effective implementation of social protection programmes. Better access to data can allow entrepreneurs to develop innovative commercial and social goods and services. A strong data governance framework can be the first step towards a future where data serves the people. If done right, such a framework enables efficient, secure and rights-based data exchanges domestically and across international borders. It ensures data privacy, establishes a data-driven culture, harnesses the value of data and leverages the potential of data to create better policies and better digital services and products.

In Türkiye, data plays an increasingly important role in development – primarily due to the increasing amount of data generation across various sectors and the evolving nature of Türkiye's data requirements. However, there are common issues: in particular data will sometimes be inaccessible to the relevant stakeholders, and different datasets do not align with one another. These challenges encompass diverse data types including administrative data, operational data, transactional data, big data, and open data. To address these data silos, there is a pressing need to promote an open data approach, to encourage reliable data sharing and to enhance interoperability. Not only is there a need to ensure that different systems can exchange data seamlessly within the data ecosystem; there is also a need to establish clear rules and regulations for data sharing and to develop technical data standards. There is a particular need to focus on big data governance for Artificial Intelligence (AI) and analytics.

In this respect, a data governance framework that defines processes for data access, usage, reusage and data sharing, and that is built on principles of protecting human rights and inclusiveness, can give a great impulse to Türkiye's digital transformation. It can shape Türkiye's digital infrastructure, including by informing the technological choices made by the public sector.

A project was designed to support Türkiye's data governance by providing expertise in the form of key policy recommendations informed by a study visit programme and by organising a workshop for stakeholders. In this way UNDP, through the CDO and UNDP Türkiye Country Office, supports the DTO in developing the conceptual framework for Türkiye's data governance. It is suggested this framework consist of a number of principles, pillars and mechanisms.

This document has been designed based on a needs assessment which found that what would be most useful was a set of recommendations and action points created through a multi-stakeholder consultation process, a review of international guidelines and country case studies. It lays the foundation for subsequent UNDP – Government of Türkiye joint projects on data governance.

The following sub-section, the latter half of section A, summarizes the methodology for the development of this report. Section B then covers the results of the fact-finding mission to Türkiye while Section C provides some key points that emerged from the review of international frameworks and the strategic documents of case study countries. Section D provides a set of recommendations and suggested action points that UNDP offers with respect to a data governance framework of Türkiye.

2. Methodology

The development process for this report[10] has the following phases:

- **Desk-based review**

UNDP conducted a desk review of existing documents and reports from Türkiye, international institutions and case study countries.

The first part was performed using information from DTO on international studies, surveys and national strategies as well as using publicly available documents on data and digitalization.

The second part further interrogated frameworks on data governance from international institutions and case study countries. This review process considered seven countries which have publicly available data governance frameworks, legislation and strategies: Germany, New Zealand, Singapore, the Republic of Korea, Switzerland, the United Kingdom (UK) and United States of America (USA). In addition to these case studies, international approaches and information originating from other countries was also considered. The list of reviewed documents and references is given in Annex 1.

- **Primary data collection and stakeholder consultations**

In May 2023, UNDP conducted stakeholder consultations to get insights on the needs, demands and use-cases from all stakeholder groups including DTO (the main stakeholder), ministries, government institutions, municipalities, universities, CSOs and the private sector in Türkiye. To ensure inclusiveness, key stakeholders were interviewed in small groups based on the roles they play in the national data ecosystem. A list of stakeholders interviewed is provided in Annex 2.

The process consisted of online meetings and face to face meetings with stakeholders. Hybrid (digital and in person) working arrangements were used. UNDP adopted an overall implementation strategy that prioritized consistent and effective coordination with interview respondents, offering flexibility to adjust to their needs and schedules.

[10] The analysis presented in this recommendation report is based on a review of existing reports, programmes and other relevant documents, spanning the working period of this report from 15 April 2023 to 30 November 2023.

There was a participatory and collaborative approach with key stakeholders at all stages. This was achieved through interactive meetings to better understand the requirements of the data governance framework. This approach opened opportunities for discussions on the process of change required to implement the framework.

UNDP conducted a series of meetings with different stakeholders with the support of DTO. Over 40 interviews and meetings were conducted using the guidance provided in Annex 3 as an interview protocol. The number of consultations by stakeholder type are given in Table 1:

Table 1. Stakeholder consultations

Agency Category	Nr. of meetings
1. Ministries and government institutions	31
2. Private Sector	4
3. Academia	3
4. Civil Society Organizations	5
Total	43

- **Data analysis and development of the data governance framework recommendation report**

This phase involved the synthesis of the qualitative data gathered so far into the information that informed the development of this report. Primary recommendations were then developed and included based upon this analysis.

The observations made in sections B and C represent a good faith attempt by the authors to summarise feedback that was received using the above methodology. That therefore does not necessarily reflect the authors' own views or the views of UNDP. Section D, the recommendations, represents the author's perspective on what actions these findings motivate.

B. Fact finding mission results

1. Overview

In Türkiye, the data ecosystem consists of many stakeholders including ministries, academia, the private sector and CSOs. Every stakeholder in the ecosystem is vital to sustain data production and utilization.

The legal landscape in Türkiye includes key legislation with respect to data, statistics and information. While the Turkish Statistical Law[11] regulates the collection, compilation, processing, and dissemination of official statistics in Türkiye, the KVKK[12] is the primary legislation governing the protection of personal data. This law regulates the processing of personal data, the rights of data subjects and the obligations of data controllers and processors. The Geographic Information Systems Law[13] focuses on standards for geographic information systems and the collection, production and sharing of geographic data. The Law on Right to Information[14] addresses the public's right to access information held by public institutions and organizations. This law does not have a specific focus on data, but does apply to data.

There is no comprehensive national data strategy in Türkiye that encompasses governance. However, its importance has been emphasized in relevant policy and strategy documents such as the 11th Development Plan[15], 12th Development Plan[16], National Artificial Intelligence Strategy (NAIS)[17], draft Public Cloud Strategy and draft Digital Government Strategy. Many of these documents have led to the adoption of relevant measures. According to the 2022 Annual Presidential Program[18], published by the Presidency of Strategy and Budget, the DTO was assigned the duty of forming a Data Governance Working Group, initiating the preparation of a National Data Strategy and providing support for data standardization and data-driven initiatives. The Data Governance Working Group has already been formed with the NAIS as its governing document. The Medium Term Program (2024-2026)[19] prepared by the Government in September 2023, the 2024 Annual Presidential Program[20] issued in October 2023 and the 12th Development Plan issued in November 2023 all include the preparation of a national data strategy as a priority.

Türkiye has already made great efforts in data governance especially after the Turkish Statistical Law was published in 2005 under the leadership and coordination of TurkStat. The governance of the Turkish Statistical System (TSS) is ensured by the Statistical Council, the Official Statistics Programme (OSP - defined by the Turkish Statistical Law) and the working groups of the OSP (consisting of producers of official statistics, representatives of CSOs and academics).

[11] Türkiye, Turkish Statistical Law (2005), https://www.tuik.gov.tr/Kurumsal/Turkiye_Istatistik_Kanunu
[12] Türkiye, Personal Data Protection Law (2016), https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law
[13] Türkiye, Geographic Information Systems Law (2020), https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=7221&MevzuatTur=1&MevzuatTertip=5
[14] Türkiye, Law on Right to Information (2003), https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=4982&MevzuatTur=1&MevzuatTertip=5
[15] Türkiye, the Presidency of Strategy and Budget, The Eleventh Development Plan (2019-2023) (2019), https://www.sbb.gov.tr/wp-content/uploads/2022/07/Eleventh_Development_Plan_2019-2023.pdf
[16] Türkiye, the Presidency of Strategy and Budget, The Twelfth Development Plan (2024-2028) (2023), https://www.sbb.gov.tr/wp-content/uploads/2023/11/On-Ikinci-Kalkinma-Plani_2024-2028_17112023.pdf
[17] Türkiye, Digital Transformation Office of the Presidency of the Republic of Türkiye, National Artificial Intelligence Strategy 2021-2025, https://cbddo.gov.tr/SharedFolderServer/Genel/File/TRNationalAIStrategy2021-2025.pdf (accessed on 21 June 2023)
[18] Türkiye, the Presidency of Strategy and Budget, 2022 Annual Presidential Program (2021), https://www.sbb.gov.tr/wp-content/uploads/2021/10/2022-Yili-Cumhurbaskanligi-Yillik-Programi-26102021.pdf
[19] Türkiye, the Presidency of Strategy and Budget, Medium Term Program (2024-2026) (2023), https://www.sbb.gov.tr/wp-content/uploads/2023/09/Medium-Term-Program-2024-2026.pdf
[20] Türkiye, the Presidency of Strategy and Budget, 2024 Annual Presidential Program (2023), https://www.sbb.gov.tr/wp-content/uploads/2023/10/2024-Yili-Cumhurbaskanligi-Yillik-Programi.pdf

From the outset meetings with the producers and users of data have been an important component of the governance of the TSS.

The Personal Data Protection Authority serves as the regulatory body responsible for personal data protection. Its role includes setting and enforcing data protection standards, guiding organizations with respect to compliance, safeguarding individuals' rights and informing the public about data privacy. The KVKK, which was published in 2016, regulates the protection of personal data.

Several ministries and institutions are also engaged by work on data governance including the Ministry of Treasury and Finance, Ministry of Environment, Urbanization and Climate Change, Ministry of Interior, Ministry of Industry and Technology and the Scientific and Technological Research Council of Türkiye (TÜBİTAK). Particularly relevant studies and projects are expanded upon below, in addition possible next steps they could take are suggested.

- By 2025 a "Public Data Space" will be established to ensure secure and reliable data governance among public institutions. It will use TurkStat's data governance infrastructure and operate under the coordination of DTO. In order to generate more value from data, activities are planned to support external participation and develop the open-source ecosystem. These activities include drafting a conceptual paper, developing reference architecture, conducting a pilot project, developing a technical system, technical and administrative capacity building work, advance data skills trainings and building a data migration programme for institutions. These activities should enhance data analytic skills in the public sector, and should extend these benefits to the private sector and academia by using sectoral data cloud platforms to set up sectoral data spaces. A planned "AI Data Governance Guide" will also shape this action.
- The Open Data Project[21] was launched under the coordination of DTO in order to share data produced by public institutions in the course of business operations and service supply in ways that respect the privacy principles of personal data, national security and trade secrets. The National Open Data Portal, which will be implemented as part of this project, is a data sharing platform that will present anonymized open government data to citizens and scientists. This should generate increased value from the data by increasing transparency, accountability, participation in government and innovation. As part of implementing this project, situation analysis studies have already been conducted. Research is ongoing and, in the meantime, DTO is coordinating a number of technical, legal and organizational processes for the dissemination of public data. The project is also currently developing data management methods, legal and administrative regulatory infrastructures and a number of guide papers.
- The National Data Dictionary Project[22]: This is an ongoing project to solve the challenges of integrating the information systems of public institutions and organizations. The dictionary will help create a common language in information systems which in turn will help resolve duplicative and conflictive data and unknown data ownership. The National Data Dictionary has started the process of standardizing data, and a Data Dictionary Portal has been established under the auspices of the DTO. It aims to:
  - compile a national data inventory,
  - identify data ownership,
  - configure management and monitoring processes through national data integration architecture,
  - ensure the use of common terminology and create corporate memory,
  - identify national data models,

[21] Türkiye, Digital Transformation Office of the Presidency of the Republic of Türkiye, Open Data Project, https://cbddo.gov.tr/en/opendata/about-the-project/ (accessed on 21 June 2023)

[22] Türkiye, Digital Transformation Office of the Presidency of the Republic of Türkiye, National Data Dictionary Project, https://cbddo.gov.tr/en/projects/nationaldatadictionary/ (accessed on 21 June 2023)

  - improve processes for new software, and
  - create a central service design platform.
- DTO is in the development phase of a new Digital Government Strategy. There will be a special focus on data governance within this strategy.
- An Information and Communication Security Guide[23] was prepared by DTO for the use of stakeholders in 2019. It includes security measures to be taken by public institutions and enterprises providing critical infrastructure services. It is the first national document in the field of information and communication security and was prepared through an extensive collaboration with relevant stakeholders. The Guide defines critical data and which security measures are appropriate for data and information of various degrees of criticality. The Guide sets out principles for the exchange of critical data internationally. The Ministry of Industry and Technology will publish further information and communication security guidelines for industry soon.
- The NAIS[24], published in 2021, covers some critical aspects of data governance as it relates to AI. An "AI Data Governance Guide" will be also developed in 2024. It will cover reference architecture (legal, technical and administrative), responsibilities and steps for implementation.
- KamuNET[25] is a closed circuit private virtual network infrastructure managed by the Ministry of Transport and Infrastructure. It provides heightened security against physical and cyber-attacks. This enables secure data exchange among public institutions in Türkiye. In 2018, public institutions started providing data from their services to the e-Government Gateway through KamuNET. The number of public institutions connected to KamuNET reached 140 by the end of 2021[26].
- The National Cyber Security Strategy and Action Plan (2020-2023)[27] was published in 2019 by the Ministry of Transport and Infrastructure, the responsible body for cyber security. This Action Plan also aims to enhance data security through various measures such as improving KamuNET and ensuring the security of internet traffic data.
- The Data Controllers Registry Information System (VERBIS)[28] was established by the Personal Data Protection Authority to promote publicly available information about data controllers, the purposes of data processing and available categories of data.
- The Electronic Data Research Center (EVAM)[29], established under the responsibility of TurkStat, is a platform that enables data analysis work by allowing authorized applications and desktop software to be accessed remotely via a web browser. It provides a fast and easily created working environment and offers several services and features that enable users to carry out their operations quickly and securely. Participants can use the EVAM Portal to query and view the datasets they are authorised to see.
- The Ministry of Environment, Urbanization and Climate Change, General Directorate of Geographic Information Systems conducted a project in support of the TUCBS[30] which aimed to establish and develop its geographic data infrastructure. Efforts are being made to

[23] Türkiye, Digital Transformation Office of the Presidency of the Republic of Türkiye, Information and Communication Security Guide, https://cbddo.gov.tr/en/icsguide/ (accessed on 21 June 2023)

[24] Türkiye, Digital Transformation Office of the Presidency of the Republic of Türkiye, National Artificial Intelligence Strategy 2021-2025, https://cbddo.gov.tr/SharedFolderServer/Genel/File/TRNationalAIStrategy2021-2025.pdf (accessed on 21 June 2023)

[25] Türkiye, Digital Transformation Office of the Presidency of the Republic of Türkiye, KamuNET Project, https://cbddo.gov.tr/en/projects/kamu-net/ (accessed on 23 June 2023)

[26] European Commission, Digital Public Administration factsheet 2022 Türkiye (2022), https://joinup.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2022_T%C3%BCrkiye_vFinal_0.pdf

[27] Türkiye, Ministry of Transport and Infrastructure, National Cyber Security Strategy 2020-2023 (2020), https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2020-2023.pdf

[28] Türkiye, Personal Data Protection Authority, Data Controllers' Registry Information System, https://www.kvkk.gov.tr/Icerik/6650/VERBIS (accessed on 30 June 2023)

[29] Türkiye, Turkish Statistical Institute, Electronic Data Research Center (EVAM), https://evam.tuik.gov.tr/ (accessed on 30 August 2023)

[30] Türkiye, Ministry of Environment, Urbanization and Climate Change, General Directorate of Geographic Information Systems https://cbs.csb.gov.tr/en (accessed on 12 July 2023)

create a portal and determine content and exchange standards so that public institutions and organizations can responsibly share geographic information through common infrastructure. As part of these efforts:
  - All geographic data in the National Geographic Data Responsibility Matrix[31] was published.
  - The Geographic Data Permissions Regulation[32] was passed to regulate the collection, production, sharing and sale of geographic data by individuals and private legal entities.
  - The Geographic Information System (GIS) Executive Board was established to monitor the implementation of specific goals, coordinate the implementation of geographic information services and review and publish documents specifying relevant standards.
- The Spatial Address Registration System (MAKS) operates under the Ministry of Interior's Directorate General of Civil Registration and Citizenship. It serves as a platform where authorized administrations across the nation, including Municipalities, Special Provincial Administrations, Organized Industrial Zone Directorates and Free Zones, work on issues of location and construction. MAKS facilitates spatial analysis by utilizing postal data and geographic coordinates.
- The Safir product, developed by TÜBİTAK, offers advanced data analytics, AI and secure data sharing infrastructure and services. Utilizing cloud infrastructure and a GAIA-X[33] and International Data Spaces (IDS) compliant architectural design[34], SafirCloud enables the development of "SafirBigData" for big data projects and "SafirIntelligence" for advanced analytics and AI projects. It also provides flexible, scalable and customizable infrastructure which can be used to solve various domain-specific problems.
- The Turkish Academic Network and Information Center[35] (ULAKBİM) provides national academic e-infrastructures that support advanced technologies, enable access to scientific knowledge, promote open-source software and develop educational technologies that serve the country's students and researchers. The Aperta Türkiye Open Archive has been established and merged with the earlier Aperta TÜBİTAK Open Archive, making its content accessible to the whole country. Designed as a data repository, the Aperta Türkiye Open Archive is a platform that maintains research data within a standardized data structure.
- The Integrated Public Financial Management Information System[36] is a project which has been launched by the Ministry of Treasury and Finance (Directorate General of Public Accounts) and has been under continuous development ever since. The Project accommodates open-source coded software architecture that support interactive processes and can share information in line with international standards. Various systems were developed under this project to allow for electronic accounting and financial transactions by public entities.
- The Entrepreneur Information System (GBS) carried out under Ministry of Industry and Technology is an enterprise-based information system that integrates data from the administrative records of 13 different institutions. Economic activity data of ventures generating commercial profits are consolidated in a central database. The purpose of GBS is to provide an environment where accurate and reliable data is presented to users (decision makers, experts and researchers) to help them in the design, implementation and measurement of the effectiveness of economic, sectoral and regional policies.

[31] Türkiye, Ministry of Environment, Urbanization and Climate Change, General Directorate of Geographic Information Systems, Mevzuat (Legislation) (2021) https://webdosya.csb.gov.tr/db/cbs/icerikler/mevzuat-kitabi-dijial-web-020721-rv-20210702093531.pdf

[32] Ibid.

[33] Gaia-X, https://gaia-x.eu/ (accessed on 30 August 2023): It enables a federated and secure data infrastructure, whereby data are shared, with users retaining control over their data access and usage. It enables the creation of links between many cloud service providers in a wider, transparent and fair ecosystem to drive the European Data economy of tomorrow.

[34] International Data Spaces Reference Architecture Model, https://internationaldataspaces.org/publications/ids-ram/ (accessed on 30 August 2023)

[35] Türkiye, Turkish Academic Network and Information Center, https://ulakbim.tubitak.gov.tr/en (accessed on 13 October 2023)

[36] Türkiye, Ministry of Treasury and Finance, Bütünleşik Kamu Mali Yönetim Bilişim Sistemi (Integrated Public Financial Management Information System), https://muhasebat.hmb.gov.tr/bkmybs-projesinin-amaci (accessed on 29 October 2023)

- The Ministry of Health developed a National Health Data Dictionary[37] with the aim of collecting, standardising, analysing and evaluating data from all healthcare institutions. This ensures the effective and reliable sharing of information between different systems.

2. Key insights

The Government of Türkiye recognizes that it is crucial to establish a data governance framework that enables the generation of public value through the use of data in an ethical way which inspires trust. There is also a willingness on the part of stakeholders to participate in the data ecosystem.

Policies, legislation and regulations

Türkiye has made progress in establishing legal frameworks to support digital transformation and data privacy. However, there are still areas that require attention to ensure compliance with international standards, to promote data sharing and to foster a data-driven culture.

- There are a significant number of pieces of legislation and regulations related to the data of public institutions. This risks the possibility of discrepancies between them which can create challenges for data access and usage.
- The KVKK serves as the fundamental legal framework for personal data in Türkiye. It outlines principles, procedures and obligations related to the processing and protection of personal data.
    - While this law provides a baseline for data protection, there is a need for its revision to ensure compliance with the EU's GDPR legislation and to address emerging challenges

[37] Türkiye, Ministry of Environment, Urbanization and Climate Change, General Directorate of Geographic Information Systems, Mevzuat (Legislation) (2021)

posed by new digital technologies. These revisions relate to revising conditions for the processing of personal data, to defining special categories of personal data and to the exchange of personal data internationally.
    - In spite of the security measures in the KVKK, institutions can be reluctant to share data. Some stakeholders need further guidelines and standards to aid their teams in comprehending their policy responsibilities in order to unleash the untapped potential of data.
    - There are a set of guidelines that are helping to inform public servants about the correct behaviours and approaches required for the ethical treatment of data. Further, the KVKK covers issues of privacy and consent around the use of personal data. However, while its provisions are powerful and reflect a well-considered understanding of the issues that need to be addressed, there is a gap between the law and its practice. Many institutions are failing to offer any mechanism for users to manage their data permissions or see a historic record of consents they have given.
    - The KVKK provides for data from different countries to be treated differently depending upon the adequacy of data protection in those countries. Countries now need to be categorised according to whether protection levels meet those thresholds. This is important as it will allow the private sector to explore international business opportunities.
- While there are existing protocols facilitating data sharing, use and reuse among government institutions, the challenge lies in the lack of standardization between these protocols. There is an overreliance on institution-dependent protocols. Addressing this issue requires a comprehensive approach involving standardization, legislative measures and the implementation of automated processes to ensure secure, efficient and uniform data sharing.
- While legislation is crucial, there is a need for additional support in terms of guidelines and standards to assist public sector teams in understanding their policy responsibilities.
    - Guidelines are missing with respect to how to access, produce and process data.
    - Guidelines should cover areas such as data collection, data sharing and data interoperability to ensure consistent practices and promote data-driven decision- making.
- Türkiye lacks a comprehensive national data strategy, which can serve as a policy framework for data governance and utilization. A national data strategy would provide a clear direction for the collection, sharing and use of data, and promote a data-driven culture across public sector organizations.

Institutions, mechanisms and processes

Türkiye is taking steps to track operational performance, ensure accountability and demonstrate a return on investment. Some stakeholders have an awareness that data can play a critical role in their work. There are ongoing projects and initiatives which different institutions within the data ecosystem are implementing. However, Türkiye faces challenges in establishing effective mechanisms and processes for data governance.

- High-level commitment is essential to drive data governance initiatives and create a data-driven culture within the public sector.
- A Chief Data Officer or a body responsible for data governance and data management in the central government does not exist. It is crucial to designate a leadership position with responsibility for data across the country to provide guidance and ensure the coordination of data governance efforts.
- There is a lack of clarity regarding ownership and accountability for the data agenda. There is also a lack of awareness of the benefits that can be obtained from data. This is leading to missed opportunities with respect to training and cultivating a data-driven mindset within the public sector.
- There is a need for clear task allocation and clarification of roles and responsibilities within

the data ecosystem. Defining roles, responsibilities and ownership of data will help avoid duplication of efforts, streamline processes and ensure accountability.

- Inadequate mechanisms for data flows pose challenges to data governance in Türkiye. Clear processes and channels need to be established to enable seamless data sharing between institutions. Additionally, there is a need to institutionalize data governance practices to ensure standardized approaches across the public sector.
- Data governance should focus on supporting decision-making through the use of data. It is important to identify and prioritize areas where data can have the most significant impact, and establish mechanisms to collect, analyse and disseminate relevant data to support informed decision-making.
- There is inadequate communication and coordination within the data ecosystem. Addressing this is crucial for successful data governance. Online systems or applications can be used to communicate and define rules and responsibilities. Regular exchange of information and best practices, and frequent collaboration can help overcome challenges and promote a culture of data sharing. This culture should include data privacy and security principles.
- The centralized national digital government platform (türkiye.gov.tr) has proven to be an effective platform for data sharing among public institutions in Türkiye. There is a web-based application (https://kamu.turkiye.gov.tr/) that works on the e-Government Gateway. It facilitates secure data sharing among public institutions through a robust infrastructure, eliminating the need for each institution to establish its own set of data connections.[38]
- Different platforms for data exchange were developed in the past to serve the needs of different organisations or groups of users. There is a need to develop more centralized and standardized platforms to facilitate efficient and secure data exchange between these organizations and users. Current practices indicate a need for greater organisation of data management, processing and storage, especially within the public sector. Only some institutions are proactively engaged in data sharing and, among those, a significant portion rely on time-consuming largely manual methods rather than efficient machine-to-machine interfaces.[39] Some organisations demonstrated a reluctance to share data due to concerns about data security.[40]
- To ensure accountability and compliance with data governance practices, the establishment of audit mechanisms is needed. Regular audits can help identify gaps, assess data quality and ensure adherence to data protection and privacy regulations.
- There may be different data maturity levels in the public sector. Some government institutions like the Ministry of Environment, Urbanization and Climate Change have data governance frameworks and some mechanisms in place, including a board and a data sharing matrix.
- Establishing sector-specific data spaces can lead to targeted and specialized data management and analysis, enabling more efficient decision-making within those sectors.
- While organizations in the public sector use data for predictive purposes in designing delivering public services and supporting financial management and budgeting, there is room for improvement. The sharing of performance data with other institutions or the public is practiced inconsistently, indicating the need for greater transparency in publishing data on the effectiveness of government services and policies.[41]

[38] Türkiye, Turksat, Turkish e-Government Gateway, https://www.turksat.com.tr/sites/default/files/2020-07/turkish-e-government-catalog-en.pdf (accessed on 30 August 2023)
[39] OECD, Digital Government Review (2023), https://www.oecd.org/gov/digital-government-review-Türkiye-assessment-and-recommendations.pdf
[40] Ibid.
[41] Ibid.

People

Effective data governance in Türkiye relies on the involvement and capacity of core individuals. Key insights with respect to this pillar are listed below:

- There is a need to define the specific roles of individuals involved in data management, data governance, data analysis and data protection within the data ecosystem. This will help avoid confusion, ensure accountability and facilitate smooth collaboration.
- Türkiye faces challenges related to human resources for data governance:
  - One challenge is insufficiently qualified IT staff at some institutions in the public sector. High turnover rates and unfilled IT posts also pose obstacles to implementing and maintaining robust data governance practices.
  - A comprehensive IT staffing strategy is needed to address these challenges and ensure an adequate workforce capable of supporting data governance initiatives.
  - IT salary policy can be also re-evaluated with consideration given to private sector and public sector averages.
  - Target staffing levels should be reviewed.
  - New working methodologies such as hybrid or remote working could be considered, and not only for IT staff.
  - A skilled workforce who understands data, its value and how to use it responsibly is needed to enable the data ecosystem. Investing in upskilling the labour force with respect to new data sources, big data and international data standards is a crucial part of developing a data-driven culture.
- In the Turkish public sector, data is utilized for various purposes including anticipating and planning, delivering services and monitoring government activity. However, there is a lack of widespread understanding and appreciation for how data generates public value.[42]
- There is a need to further enhance knowledge and awareness of personal data protection among individuals involved in data governance. Insufficient knowledge on personal data regulations, such as the KVKK, can lead to non-compliance and potential data breaches. Some data currently cannot be shared with government institutions either as a matter of policy or because of concerns held by relevant staff. There are remarkable efforts by responsible institutions to increase awareness through guidance and training activities. These programmes should be continued to ensure understanding from a greater number of stakeholders. Staff working in the data ecosystem need further information, particularly information they can make practical use of in their daily work.
- Training and resources should be provided to equip public servants in balancing data value and public trust. Turkish public servants require training to protect privacy while making the best use of data.
- There is a lack of information on the availability of specific datasets within the data ecosystem. It is important to develop catalogue applications, and comprehensive reference materials that notify users of the types of data available, their sources and their potential uses. Challenges exist in moving towards a data-driven public sector, including some issues related to data sharing and a primary focus on individual institutions rather than considering the potential benefits of pooling data across the entire public sector. The latter would provide greater benefit – including to individual institutions.
- Many organizations are leveraging data in real-time to better serve the public. Benefits include improving emergency response, increasing engagement with the public and freeing up public servant capacity for other priorities. However, practical limitations hinder the effectiveness of organizations in taking advantage of these opportunities. These limitations stem from skill gaps and a lack of priority given to developing baseline data skills among all public servants.
- Enhancing data skills across the public sector is crucial for improving services, whether by enhancing statistical understanding or in using data to prioritize service delivery.[43]

[42] Ibid.
[43] Ibid.

Technology and infrastructure

There is high awareness of the need to develop the infrastructure to connect stakeholders. Part of creating a strategic approach to the governance of data involves being able to understand and identify the sources and flows of data. There have been initiatives to establish base data registries but only a third of organisations are actively maintaining a data inventory or data catalogue. Therefore, taking steps to improve the cataloguing and indexing of data in the Turkish public sector is important, and would help to reduce duplication, improve data quality and allow for the exploitation of opportunities to enhance the analysis and application of data.

- Challenges exist regarding data standards and interoperability. It is crucial to establish and adhere to common data standards, particularly with respect to unit and variable definitions.
- Guidelines, common sources and technological tools are needed for the software development process in the public sector. Adequate time and resources should be allocated for software development, with consideration given to the complexity of data systems and the need for them to be robust. Unrealistic demands in terms of software development can impede effective data governance.
- Many public institutions in Türkiye do not utilize cloud storage solutions, which can limit the scalability and accessibility of data. Cloud technologies can provide cost-effective and secure storage options, facilitating efficient data management due to the costs of servers. Beyond investment, cloud adoption requires adhering to globally accepted international standards, codes of conduct and best practice examples and guidelines to benefit from global know-how in this field.
- Establishing clear authorization mechanisms for data systems is necessary. Access controls and authorization frameworks should be implemented to ensure appropriate access to data, protecting sensitive information and maintaining data security.
- Inconsistencies in administrative registers, including location data, need to be addressed to ensure data integrity and reliability. Data held in relevant administrative registers must be kept up to date.
- There is a demand for data management centres and a centralized data hub to create a single system that integrates various data sources. Creating user friendly data portals can improve data accessibility, facilitate faster solutions, foster partnerships with the private sector and enable advanced data analytics.
- Utilizing web services allows stakeholders to share data efficiently, enhancing data accessibility. Automatic updating of web services by all stakeholders is an important part of the deployment of these tools.

- Standardization is seen as one of main challenges for effective data sharing. Inconsistent data validation, the lack of a single sharing point for all government institutions and communication gaps were also identified as challenges.
- The majority of stakeholders lack a robust metadata system. Improving metadata systems within institutions will enhance data discoverability and understanding while the absence of technical metadata damages efficiency. Data sharing protocols between stakeholders should ensure that the approach taken towards metadata is compliant with the concept of privacy-by-design.
- VERBIS is a system that promotes transparency by making information about data controllers, the purpose of data processing and the categories of data used publicly available. This provides a valuable first step towards transparency and accountability, but there is still a need to maintain focus on creating systems and tools that empower the public to manage their consents, including by revising laws and regulations.
- Privacy impact assessment tools should be developed to ensure compliance with data protection laws. This allows organisations to meet regulatory requirements, and also fosters a culture of responsible and ethical data handling. This in turn promotes trust among stakeholders and customers alike.[44]
- There is a need to eliminate human based errors in data management and analytics.

Partnership

The government of Türkiye is participating in collaborative efforts with various stakeholders:

- There is a national open data portal which will be implemented as part of the Open Data Project managed by DTO; this will enable faster data sharing and collaboration with the private sector and other stakeholders.
- Although there are some projects and activities involving stakeholders in the data ecosystem, partnerships with the private sector, CSOs and academia need to be strengthened to develop innovative solutions and data analytic capabilities. Public-Private Partnerships should be considered to leverage private sector data for the benefit of the public.
- Leveraging big data requires a skilled labour force. Collaboration with universities can foster the development of data analytic skills in the public sector and provide access to experts in data science and analysis.
- Collaborating with the private sector and academia on joint data projects can lead to the creation of innovative solutions, data-driven insights and the development of new technologies.
- The Public Data Space project can serve as a platform for open, secure and reliable data sharing and collaboration among various actors, including the public sector.

[44] Ibid.

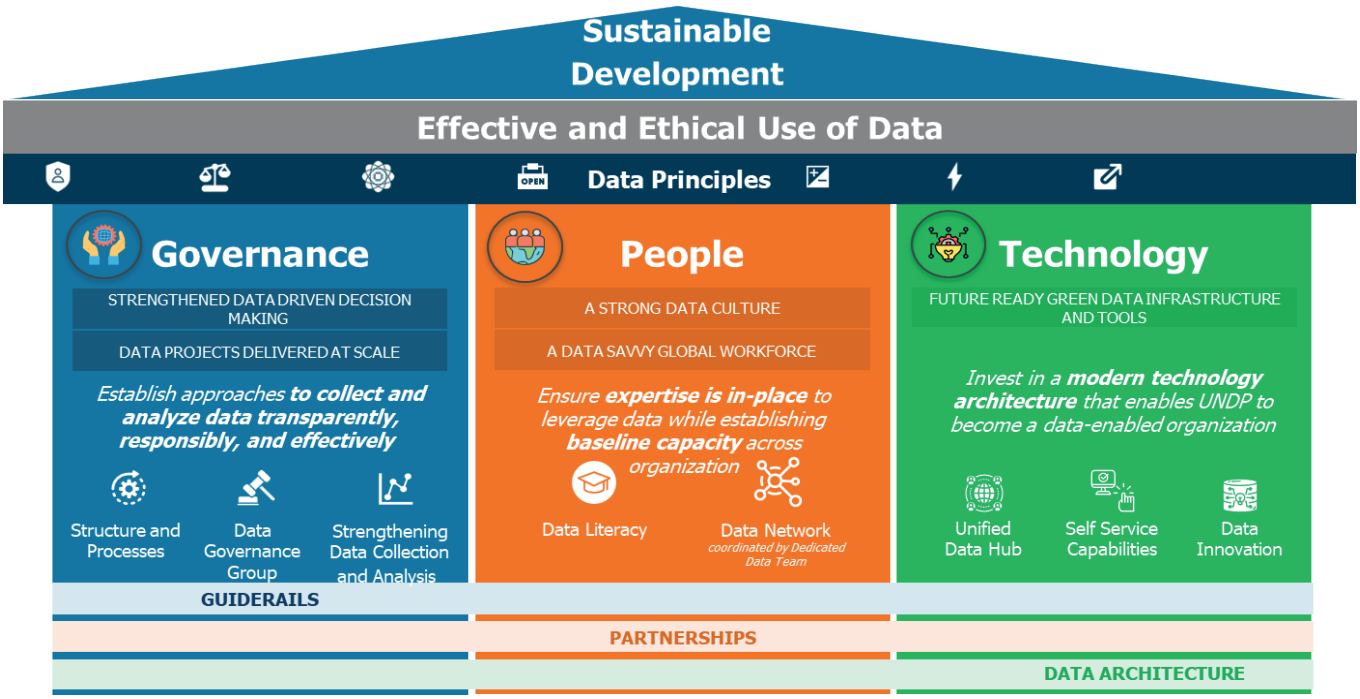
C. Review of country cases and international guidelines

1. International frameworks and guidelines

There are a variety of data governance frameworks that are used in the international context. Some examples are given below:

UNDP's Data Strategy emphasizes data as a valuable strategic asset that should be shared among stakeholders. Its framework promotes the effective and ethical use of data through three key pillars: data governance, people and technology. By strengthening these pillars, UNDP aims to enhance data management and analytical capabilities, resulting in the development of innovative services and products. This supports data-driven decision-making and evidence-based programming. The framework serves as a valuable source of inspiration for policymakers seeking to transform their departments, organizations or institutions by leveraging data-driven insights and improving the quality of decision-making processes. UNDP's eight Data Principles[45] provide additional guidance on how to ethically bring data governance to life.

Figure 1. UNDP Data Strategy



Source: UNDP[46]

In addition to these Principles, a Guidance Note published by the UN Office of the High Commissioner for Human Rights (OHCHR) provides an underlying set of principles that a human rights-based approach to data must consider (Box 1).

[45] UNDP, Data Futures Exchange, 8 Data Principles for UNDP, https://data.undp.org/who-we-are#principles (accessed on 19 May 2023)
[46] UNDP, UNDP Data Strategy (2022-2025) 2022

Box 1. A human rights-based approach to data[47]

The UN Office of the High Commissioner for Human Rights (OHCHR) developed a guidance note which outlines a Human Rights-Based Approach to Data (HRBAD) in the context of the 2030 Agenda for Sustainable Development. It offers preliminary principles and recommendations for a HRBAD, categorized under the following key headings:

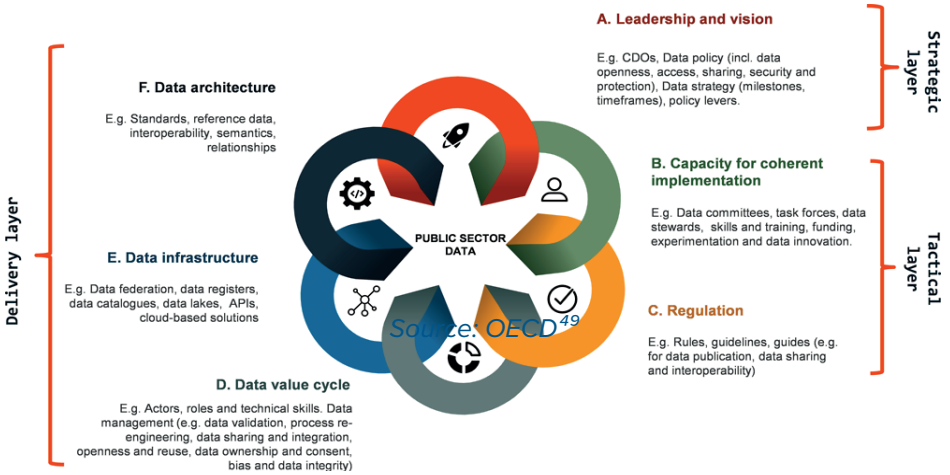
- **Participation**: Encourages active involvement of relevant stakeholders to enhance data quality and relevance, aligning with human rights norms and principles.
- **Data disaggregation:** Emphasizes the importance of breaking down data into specific categories to prevent anyone from being left behind in the pursuit of Sustainable Development Goals.
- **Self-identification:** Recognizes the value of individuals being able to self-identify and provide information about themselves in data collection processes, respecting their rights and privacy.
- **Transparency:** Calls for clear and open information sharing in data collection and usage, promoting accountability and adherence to human rights principles.
- **Privacy:** Acknowledges the need to safeguard individuals' privacy rights when collecting and handling data, ensuring their protection.
- **Accountability:** Highlights the importance of holding data collectors accountable for upholding human rights principles throughout the data collection process.

These principles and practices aim to guide data collection efforts in a manner that aligns with human rights and contributes to the achievement of the 2030 Agenda's Sustainable Development Goals while ensuring that no one is left behind.

[47] UN Human Rights Office of the High Commissioner (OHCHR), Human Rights-Based Approach to Data (HRBAD) (2018), https://www.ohchr.org/sites/default/files/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf

OECD's Data Governance in the Public Sector framework provides a universal model for data governance and has three core layers: strategic, tactical and delivery. The benefits of this framework include the fact that it covers all aspects of successful data governance, including organizational, policy and technical elements. This model is therefore especially suited for doing a "gap-analysis" of current data governance mechanisms, to newly define a framework or to adopt the specific elements and tools that fit a certain context.[48]

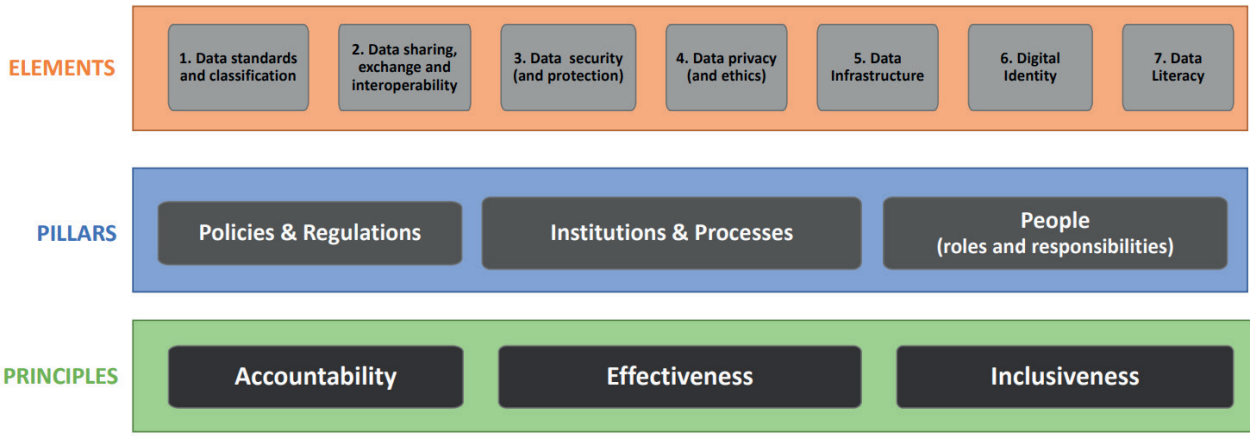
Figure 2. OECD's Data Governance in the Public Sector framework



Source: OECD[49]

UN DESA's Adopting National Data Governance Framework[50] provides a clear view of the elements, pillars and principles that make up the structure of a good data governance framework. This resource also emphasizes the importance of core principles such as accountability, effectiveness and inclusiveness in data governance. Data inclusiveness, for instance, could entail specific guidelines on how the workforce, and data collection and processing efforts, should reflect the experiences of everyone in society. This framework is a good starting point for policy makers who are looking to introduce data governance mechanisms into environments which would benefit from an easy-to-understand system or where there is currently little in place.[51]

Figure 3. UN DESA's Adopting National Data Governance Framework

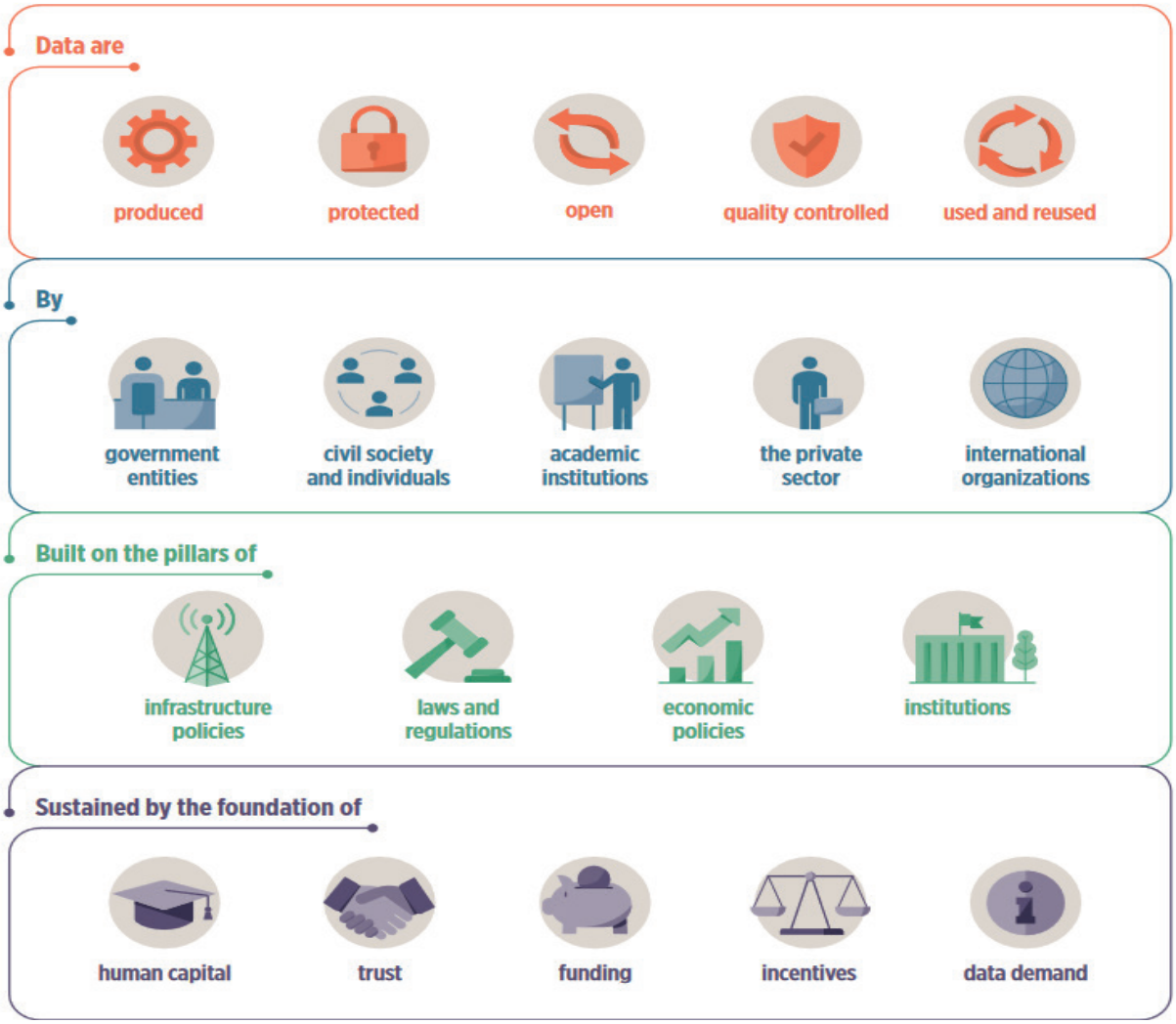


Source: UNDESA[52]

[48] UNDP, Data to Policy Navigator (2023), https://www.datatopolicy.org/
[49] OECD, Digital Government Review of Argentina (2019) https://www.oecd-ilibrary.org/governance/digital-government-review-of-argentina_354732cc-en
[50] UN DESA, Adopting National Data Governance Framework for Sustainable Development (2022), https://publicadministration.un.org/Portals/1/Adopting%20National%20Data%20Governance%20Framework%20-%20W%20Kwok%20July%202022%20FINAL.pdf
[51] UNDP, Data to Policy Navigator (2023), https://www.datatopolicy.org/
[52] UN DESA, Adopting National Data Governance Framework for Sustainable Development (2022), https://publicadministration.un.org/Portals/1/Adopting%20National%20Data%20Governance%20Framework%20-%20W%20Kwok%20July%202022%20FINAL.pdf

The World Bank's Integrated National Data System, contained within the World Development Report, offers a framework for countries to realize the full value of data for development; ensuring trustworthy and equitable production, flow and use of data. This integrated data system assumes that data governance will be undertaken using a collaborative multi-stakeholder approach, integrating participants from civil society as well as the public and private sectors into the governance structures of the system. It explicitly builds data production, protection, exchange and use into planning and decision-making. This framework is less applicable to the needs of specific departments or organizations, but rather provides guidance for a national data strategy at the state government level for states looking to capture greater economic and social value from data. For policy makers, it can serve as inspiration for how to incorporate various stakeholders into governance systems.[53]

Figure 4. World Bank's Integrated National Data System

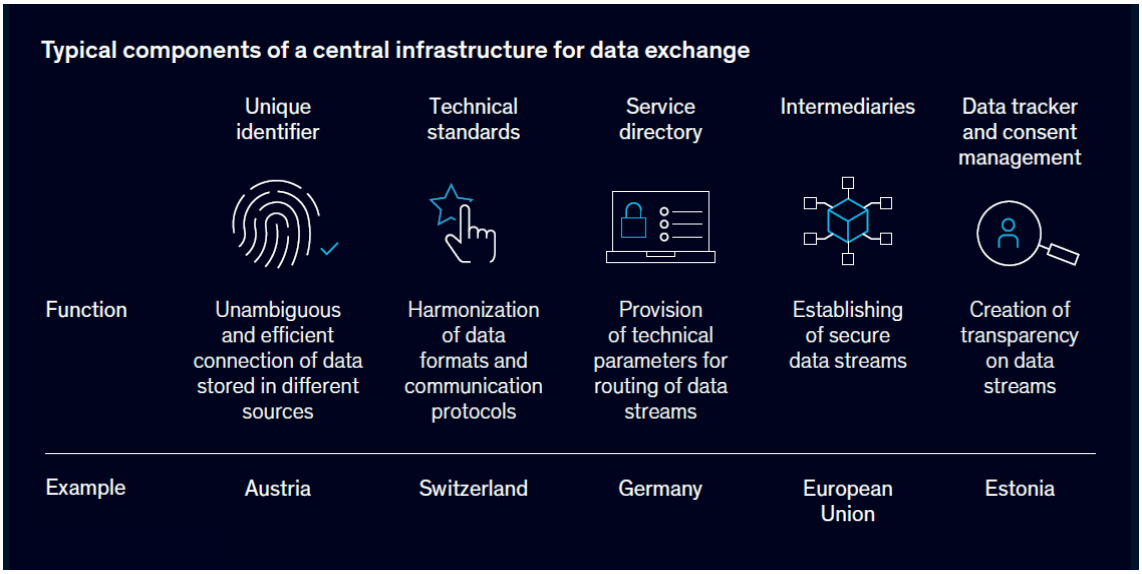


Source: World Bank[54]

Lessons from Europe: A central agency can run central data architecture, thereby establishing a common data-exchange infrastructure. This creates standardized components that are useful across a range of use cases. This means that government data can be de-siloed and be made interoperable at scale. A study by McKinsey[55] highlighted five specific components a central data architecture requires:

[53] UNDP, Data to Policy Navigator (2023), https://www.datatopolicy.org/
[54] World Bank, World Development Report 2021: Data for Better Lives (2021), https://www.worldbank.org/en/publication/wdr2021
[55] McKinsey, Government data management for the digital age (2021), https://www.mckinsey.com/industries/public-sector/our-insights/government-data-management-for-the-digital-age

Figure 5. A study by McKinsey[56]



Source:McKinsey

Since 2016 the EU has had GDPR legislation which protects natural persons with regards to the processing of personal data and the free movement of such data. GDPR sets the legal framework and requirements for the handling and protection of personal data. This in turn necessitates strong data governance to provide the structure, processes and policies that ensure compliance with these regulations.

GDPR demands the further reinforcing of data governance. For data spaces to become operational, organisational approaches and structures (both public and private) need to enable data-driven innovation that is compatible with this legal framework. GDPR also addresses the need to strengthen governance mechanisms at the EU level and in Member States. This is relevant for data use in common sectoral data spaces, for cross-sectoral data use and for data use by both private and public players.

Preparing for GDPR could include adopting a mechanism to prioritise standardisation activities. A more harmonised description and overview of datasets, data objects and identifiers will foster data interoperability between and within sectors. This can be done in line with the principles of Findability, Accessibility, Interoperability and Reusability (FAIR) of data and can take into account the decisions of sector-specific authorities.

GDPR includes sections regarding facilitating decisions on what data can be used, how and by whom for scientific research purposes. This is particularly relevant for publicly held databases with sensitive data not covered by the Open Data Directive. It can make it easier for individuals to allow the use of the data they generate for the public good.

In addition to the GDPR, the EU has developed a Data Strategy, Data Governance Act and Data Act[60]:

[56] Ibid.
[57] European Union, GDPR (2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
[58] European Union, Data Strategy (2020), https://eur-lex.europa.eu/legal-content/EN TXT/?uri=CELEX%3A52020DC0066
[59] European Union, Data Governance Act (2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868
[60] European Union, Data Act (2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN

Figure 6. EU's Data Strategy, Data Governance Act and Data Act

Source: Cyber Risk GmbH[61]

The Data Governance Act, presented in November 2020 and agreed upon by co-legislators in November 2021, creates processes and structures to facilitate data sharing by companies, individuals and the public sector. The Data Act clarifies who can create value from data and under which conditions. The Data Act removes barriers to access data for both the private and the public sector, while preserving incentives to invest in data generation by ensuring balanced control over the data. This was the next logical step after the European Data Governance Act. The Data Act was the second main legislative initiative following the February 2020 EU Data Strategy, which makes the EU a leader in the development of a data-driven society.

The Data Act gives individuals and businesses more control over their data through a reinforced data portability right. This facilitates copying or exchanging data easily across different services, which is particularly important when data generation occurs through machines and other "smart" devices.

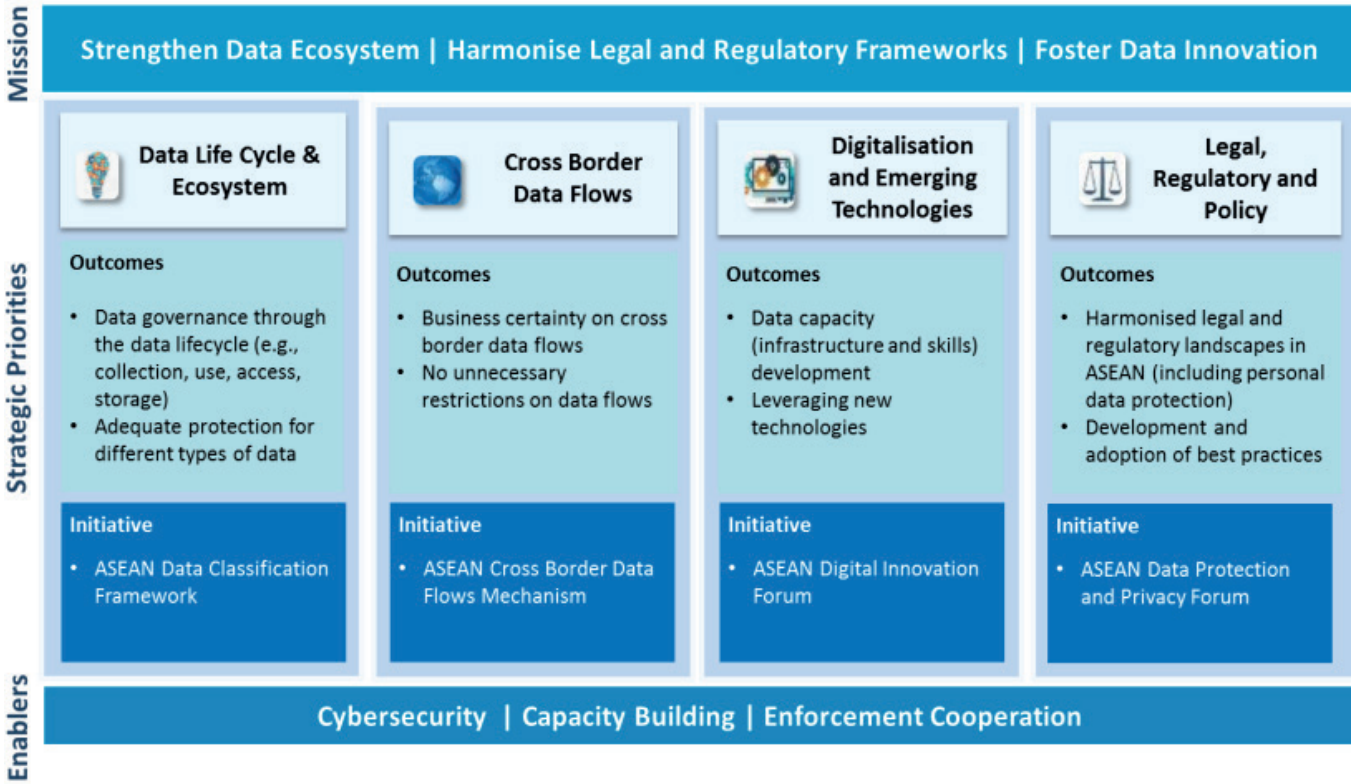
For example, a car or machinery owner could choose to share the data they generate with its insurance company. Such data, aggregated across multiple users, could also help to develop or improve other digital services, including those that monitor traffic, or identify areas at high risk of accidents.[62]

[61] Cyber Risk GmbH, The European Data Act (2023), https://www.eu-data-act.com/

[62] Ibid.

Association of Southeast Asian Nations (ASEAN) Framework on Digital Data Governance:[63] Heads of State of ASEAN Member States have agreed on a number of key deliverables for ASEAN such as cybersecurity cooperation, personal data protection and promoting innovation and e-commerce. The Master Plan on ASEAN Connectivity 2025 also identified the development of an ASEAN Framework on Digital Data Governance as an initiative that is intended to enhance data management, facilitate the harmonisation of data regulations among ASEAN Member States and promote intra-ASEAN flows of data. This will help to ensure that ASEAN, collectively realizes the potential benefits of data, with due regard given to the fact that the ten ASEAN Member States are currently at different levels of data maturity.

Figure 7. ASEAN Framework on Digital Data Governance



Source: ASEAN[64]

[63] Association of Southeast Asian Nations (ASEAN), Framework on Digital Data Governance (2021), https://asean.org/wp-content/uploads/2021/08/ASEAN-Data-Management-Framework.pdf

[64] Ibid

2. Germany

Germany has a well-established data governance framework which helps to ensure the responsible and secure handling of data.

Policies, legislation and regulations

The key elements of Germany's approach to these issues are outlined below:

- The Data Strategy of the Federal German Government[65] states that regulation needs to be differentiated and requirements-based. This is necessitated by the large number of different data sources, stakeholders and forms of use. They recommend taking steps to further reduce legal uncertainty, especially through non-legislative measures, and so establish standardised data protection practices.[66]
- The Federal Data Protection Act is the primary legislation in Germany for data protection and governs the collection, processing and use of personal data. It aligns with the EU's GDPR and provides guidelines for data governance, including: consent, data minimization, purpose limitation and data subject rights.[67]
- Germany hopes to achieve harmonization of European data protection through the ePrivacy Regulation, which focuses on enhancing privacy protection in electronic communication.[68]
- Certain industries in Germany have additional specific data governance requirements. For example, the financial sector is governed by regulations such as the Banking Act and the Payment Services Supervision Act.[69] These regulations outline further data protection and security measures that financial institutions must adhere to.
- Various industry associations and organizations in Germany have developed codes of conduct and certifications related to data governance. These voluntary frameworks provide guidelines and best practices for data handling, security and privacy.
- Germany has regulations in place to govern the exchange of personal data to countries outside the European Economic Area. These measures, such as Standard Contractual Clauses and Binding Corporate Rules, ensure that data exchanges comply with GDPR requirements.
- Germany places a strong emphasis on data ethics, and organizations are encouraged to consider ethical principles when handling data, particularly in areas like AI and machine learning.[70]

---

65 Germany, Data Strategy of the Federal German Government (2021), https://www.bundesregierung.de/resource/blob/998194/1950610/bf3dac46be741dfd4616cb56ff4e5f20/datenstrategie-der-bundesregierung-englisch-download-bpa-data.pdf?download=1

66 Ibid

67 Germany, Federal Ministry of Justice, Federal Data Protection Act (2017), https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html

68 Germany, Data Strategy of the Federal German Government (2021), https://www.bundesregierung.de/resource/blob/998194/1950610/bf3dac46be741dfd4616cb56ff4e5f20/datenstrategie-der-bundesregierung-englisch-download-bpa-data.pdf?download=1

69 Germany, Cloud Compliance Center (2023), https://resourcehub.bakermckenzie.com/en/resources/cloud-compliance-center/emea/germany

70 Germany, Data Strategy of the Federal German Government (2021), https://www.bundesregierung.de/resource/blob/998194/1950610/bf3dac46be741dfd4616cb56ff4e5f20/datenstrategie-der-bundesregierung-englisch-download-bpa-data.pdf?download=1

Institutions, mechanisms and processes

- Data protection is supervised in Germany by the Federal Commissioner for Data Protection and Freedom of Information (responsible for, among other things, federal authorities, financial authorities (in terms of personal data processing in the application of the German Fiscal Code), telecommunication companies and postal service providers) and 17 federal state officers for data protection, who supervise state-specific compliance. Together they form the Conference of the Independent Data Protection Authorities of the Federal Government and the Länder, which is designed to promote standardisation in the legal interpretation applied by supervisory authorities. Nevertheless, legal interpretations may still be divergent. This body therefore continues to consider whether and in what form improvements are needed in the coordination of standardised implementation of data protection law.
- The Federal Ministry of the Interior, Building and Community is responsible for formulating data governance policies, including data protection and data security measures. It plays a significant role in shaping the overall data governance landscape in Germany.[71]
- Germany has several data protection authorities at both the federal and state levels. These authorities oversee and enforce data protection laws, provide guidance to organizations and handle complaints related to data privacy and security.
- Germany has developed a National Strategy for AI[72] that includes data governance considerations. It focuses on fostering innovation while ensuring ethical and responsible AI development. The strategy emphasizes data protection, privacy and the transparent and accountable use of data.
- The Data Strategy of Germany also highlights the importance of data governance, the need for specialized roles and units and the need for the establishment of standardized processes to enhance data utilization, transparency and accountability. There continue to be unmet needs:
  - The German government has implemented data labs within each ministry, pioneering their approach to data governance.
  - Public administration lacks dedicated staff for data content work, with few federal ministries having a visible data team responsible for data science and/or data governance.
  - Standardized processes and roles with respect to data content work only exist in isolated cases within the federal administration.
  - The complexity of internal assessment documents and their corresponding funding measures necessitate improvements in their design and classification, including through visualization of data analysis where appropriate.
- The Federal Ministry of Defence and the Federal Foreign Office have already taken steps towards internal data governance including the appointment of a chief data officer and the establishment of data science competence centres.[73]

[71] Germany, Federal Ministry of the Interior, Building, and Community, National data protection law (2023), https://www.bmi.bund.de/EN/topics/it-internet-policy/data-protection/data-protection-node.html

[72] Germany, Federal Government, Artificial Intelligence Strategy of the German Federal Government (2020), https://www.ki-strategie-deutschland.de/files/downloads/Fortschreibung_KI-Strategie_engl.pdf

[73] Germany, Data Strategy of the Federal German Government (2021), https://www.bundesregierung.de/resource/blob/998194/1950610/bf3dac46be741dfd4616cb56ff4e5f20/datenstrategie-der-bundesregierung-englisch-download-bpa-data.pdf?download=1

People

- The Data Strategy of Germany also states that companies should design all their digital processes and services so that they are user-friendly, fair and transparent. Important mechanisms to protect citizens are provided for under data protection law and under regulations on consumer protection and protection of minors in the media. However, to increase confidence in the process, consumers should be given a better overview of how companies deal with their personal data.
- The Data Strategy suggests adding contractual regulations to the German Civil Code to strengthen the position of consumers in cases where digital products are provided to consumers without payment but where consumers provide or undertake to provide personal data.
- Germany aims to support informed handling of data by citizens of all age groups through the provision of various formal and informal educational opportunities. By doing so, they want to facilitate participation in the data ecosystem and awaken interest in developing data-driven business models. They also want to promote the collection of open data by citizens, encourage active discussion around data use within the framework of citizen-led science projects and train citizens to become experts. In short: they want to strengthen the population's data skills and will conduct a comprehensive survey to determine the extent to which they have done this.
- The Data Strategy states that all school pupils should learn how to collect, process, critically assess and use data. Data skills should be anchored in state syllabuses and prepared in an age-appropriate format. The aim is to ensure that everyone who completes a vocational training course or a degree is also taught data skills to a specified minimum standard.
- Due to changed requirements in industry, more and more companies need their employees to have data skills. Germany aims to consistently counter the increasing shortage of skilled workers by providing basic and further training for future data experts at the highest international level. They particularly want to help companies access the potential of data-based value creation. They therefore support companies in training their employees in high demand data skills.
- Civil organisations play an important role in improving data skills in Germany. The Federal Ministry of the Interior, Building and Community will continue funding and supporting civil organisations that teach data skills to German citizens.
- Efforts are underway to enhance the data skills within the federal administration by creating new positions, responsibilities and units focused on data-based work. Most government authorities have data protection officers but lack a chief data scientist or chief data officer responsible for data governance and enabling further data utilization. The strategy points out that establishing a chief data scientist role can promote better data usage by federal authorities, increase the availability of open data and identify areas for improvement.[74]

Technology and infrastructure

- A large number of public and private data infrastructures have been established over the past few years in Germany, each with their own standards and framework conditions for users. A wide range of projects are underway in science and industry. The landscape is very fragmented and continually changing. This is why the National Research Data Infrastructure was established. This will be supplemented by a research data action plan, which combines activities on improving the use and usability of research data, and aims to promote cultural change in science in favour of strengthening data sharing and reuse behaviours.

[74] Ibid.

- There is also a local network of 34 accredited research data centres. These serve to improve access for the science sector to microdata from research and from official statistics.
- GAIA-X is a project that aims to link up local infrastructure services (particularly cloud and edge solutions) to form a user-friendly system.
- The European Open Science Cloud is moving into the implementation phase and is creating a Europe-wide, trustworthy, virtual networked environment in which research findings can be stored, shared and reused digitally. Progress towards this continues in Germany.
- Germany is committed to the development of universal standards of data quality, metadata and the interpretability of data held in the National Research Data Infrastructure. A particular priority is interoperability with data in the European Open Science Cloud and consideration of standards for the digital representation of measurement data established by the Meter Convention (the International Committee for Weights and Measures).
- As part of a new framework programme on microelectronics, Germany will promote electronics for energy-saving ICT and data processing.
- Germany's data strategy also includes the idea that cross-departmental data infrastructure, such as a data analysis platform accessible to the entire Federal Government, should be developed. This infrastructure should integrate with existing infrastructures to avoid duplicating efforts.[75]

Partnerships

- Within the framework of Germany's partnerships with developing countries and emerging markets, the nation plans to examine the extent to which the potential of satellite remote sensing can be tapped to support sectors including agriculture. For example, open data and AI can be used for better monitoring of harvests and yields.
- Germany's Data Strategy states that trustworthy intermediaries can make an important contribution to ensuring access to data and data exchange and to reinforcing a decentralised, sovereign data economy. Data trustees are good examples for these. Data trustees can simplify and facilitate data sharing through various structures, such as by providing infrastructure and ensuring compliance with current data protection laws, or by performing anonymisation procedures.
- Data trustees can also consolidate expertise, ensure the quality of the data records, manage access rights or guarantee compliance with universal standards. Finally, data trustees can also operate in the interests and for the protection of consumers, including in relation to personal data. However, these different forms of data trustees have not yet become established in the data ecosystem to an extent which would allow upscaling.
- Non-personal data is still not used or shared enough in Germany. Many companies state that they perform data exchanges, but they usually only mean exchanges within their network of customers or suppliers. Innovative data partnerships can be specifically promoted by new stakeholders in the data ecosystem.
- There are a number of different types of data partnerships. All require participants to have mutual trust in the quality and integrity of data. Germany wants to create data quality metrics which show the various levels of anonymisation that can be guaranteed by data trustees. The establishment of synthetisation and verification servers could help to make this a reality.[76]

[75] Ibid.
[76] Ibid.

3. New Zealand

The data governance framework of New Zealand is designed to ensure the effective and responsible management of data across government agencies. The New Zealand model is based on the understanding that data and information governance efforts may face cultural, political and organizational challenges, leading to resistance to necessary changes. It proposes the following responses:

- Take a holistic approach to data and information governance, which addresses people, politics and culture before addressing processes, stewardship and technology. Progress gradually up the maturity scale while balancing strategic objectives with tactical compromises.
- Obtain executive support for data and information governance. Make clear it involves behavioural and cultural changes as well as funding and technology investments. Align with key decision makers.
- Define data stewardship early on, ensuring effective control and use of data and information assets. Build a data steward team comprised of subject matter experts from all business areas. Consider the need for creating official positions within a given agency based on that agency's stage of development and cultural environment.
- Establish quantifiable benefits through a business case, highlighting the long-term advantages of an effective data and information governance program. Calculate the cost of managing data, quantify business risks and identify revenue opportunities through improved customer service and analytical insights.
- Establish, collect and report on metrics to measure progress in data and information governance. Focus on quantitative metrics that align with project objectives and overall programme goals. Consider metrics related to data and information value, management cost, decision-making and process maturity. Use a data and information governance key performance indicators dashboard to automate reporting.
- Link incentives to key performance indicators to encourage ongoing participation in the process. Integrate data measures with agency-wide key performance indicators and use them as a basis for IT investment.[77]

Policies, legislation and regulations

- **Oversight:** The New Zealand Government Chief Data Steward[78] oversees the implementation of this framework, which provides guidance and standards for data governance practices across government agencies. It establishes principles and best practices for data management covering areas such as data quality, data sharing, privacy, security and ethical use of data.[79]
- **Data Privacy and Protection**[80]: New Zealand has robust privacy laws in place to protect personal information. The Privacy Act 2020 sets out principles for the collection, use and disclosure of personal data. Agencies are required to adhere to these principles when handling personal information.

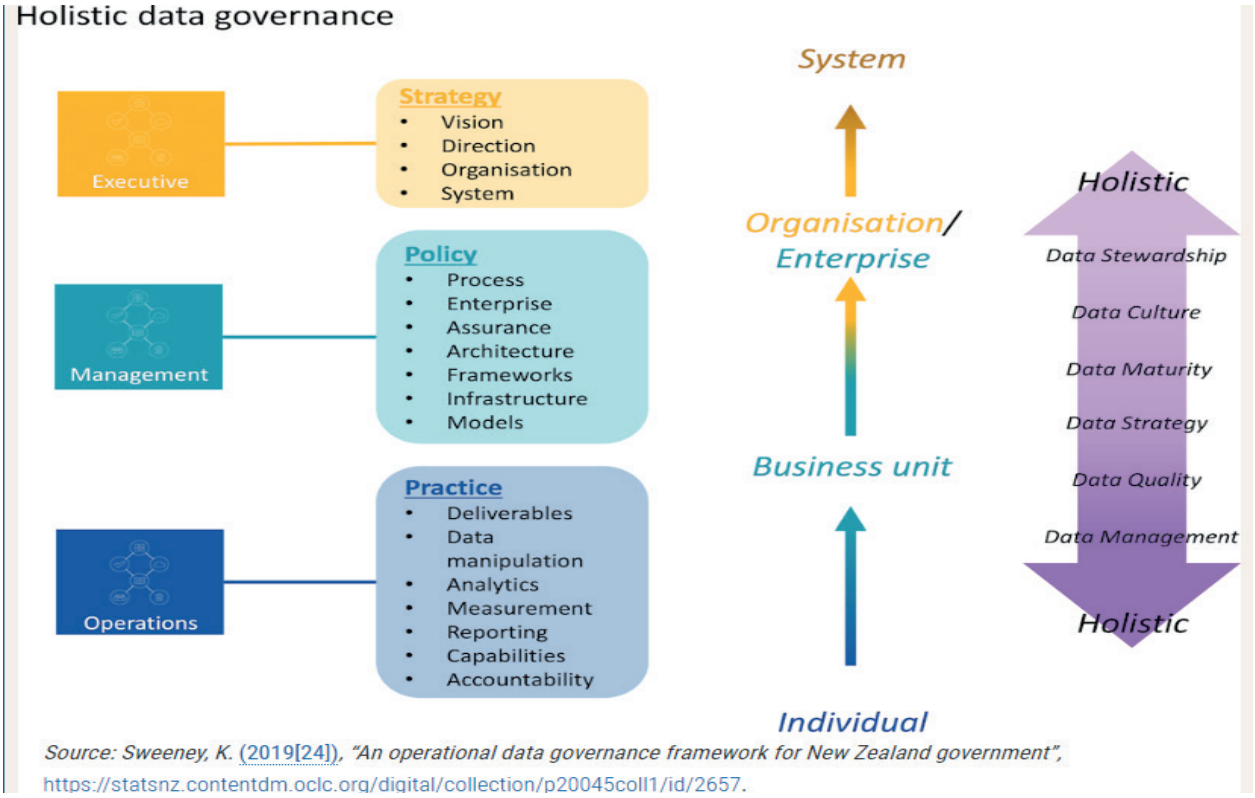
[77] Ibid.
[78] New Zealand, Department of Internal Affairs, Data and Information Governance Toolkit Guidelines (2015), https://www.digital.govt.nz/assets/Standards-guidance/Technology-and-architecture/Architecture-Resources/Data-and-information-goverance-and-maturity/Data-and-Information-Governance-Toolkit-Guidelines.pdf
[79] New Zealand, Government Chief Data Steward (2023), https://data.govt.nz/leadership/gcds/
[80] New Zealand, Department of Internal Affairs of the New Zealand, Data and Information Governance (2017), https://www.digital.govt.nz/assets/Standards-guidance/Technology-and-architecture/Architecture-Resources/Data-and-information-goverance-and-maturity/Data-and-Information-Governance-v2.2.pdf

- **Data Ethics**[81]: New Zealand recognizes the importance of ethical data use and of managing risks associated with data. Ethical guidelines are in place to ensure that data is used in a responsible and accountable manner, and agencies are required to conduct risk assessments to identify and mitigate potential data-related risks.

Institutions, mechanisms and processes

- New Zealand has established formal leadership roles within existing administrative structures. The role of Government Chief Data Steward is held by the Chief Executive of Statistics New Zealand. New Zealand's approach is noteworthy for its emphasis on policy accountability. For instance, Statistics New Zealand routinely issues a quarterly dashboard that outlines their achievements and responsibilities.
- Statistics New Zealand developed a new and improved data governance framework for the New Zealand government. The framework is part of the agency's numerous efforts to promote better data management practices across the public sector, and to leverage data as a strategic asset for decision making. One of the central pillars of the framework is the adoption of a so-called "whole-of-data life cycle approach", meaning public bodies and employees are encouraged to think more strategically about the governance, management, quality and accountability of their data over the whole of a piece of data's life cycle (i.e. from the design and source of the data to its storing, publication and disposal).[82]

Figure 8. New Zealand's holistic data governance



Source: OECD[83]

[81] New Zealand, Privacy Act (2020), https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html?search=ts_act%40bill%40regulation%40deemedreg_privacy_resel_25_a&p=1#LMS23417
[82] New Zealand, Data Ethics (2023), https://data.govt.nz/toolkit/data-ethics/
[83] Ibid.

People

- A capabilities mapping captures how an organisation does its work and what it is good at. An organisation operating with a well-defined and thoroughly integrated set of capabilities can enjoy a host of beneficial outcomes, including better performance, higher market valuations and a competitive operating advantage. The data governance framework being implemented in New Zealand considers the following set of capabilities:
  - Data point of contact.
  - Subject matter expertise.
  - Access control.
  - Risk management.
  - Internal relationship management.
  - External relationship management.
  - Quality assurance/quality control management.
  - Data management.
  - Data championship.
  - Data innovation.
- An inventory of capabilities in and of itself provides no measurable data governance benefit without a viable option to implement them amongst staff with data responsibilities. This inventory therefore needs to be integrated into the human resources system. This paves the way for good data practice to become standard, with all staff assuming accountability for data assets under their care a matter of course. A sense of ownership and improved engagement with the organisation's data assets ensures that staff consider data governance to be just another element of their normal duties.[84]

Technology and infrastructure

Building the infrastructure that enables effective data management and reuse is one of the main components of the New Zealand Government Data Strategy and Roadmap[85]. This component covers the following initiatives:

- Develop a strategic response and seek investment for the future of integrated data:
  - To respond to evolving system needs and to improve data equity by ensuring inclusive access to existing integrated data services, New Zealand will articulate investment priorities for integrated data products such as the Integrated Data Infrastructure and data lab service.
- Develop system architecture:
  - System architecture defines the structure and behaviours of a system and can be designed to ensure these align with an inclusive set of design and operational principles. Work is underway to co-design and develop a data system architecture that supports interoperability and appropriate sharing and use of data, information, and analytics.
- Confirm feasibility of a joint property data source:
  - Research is underway into the possibility of the co-development of an authoritative property data source by Statistics New Zealand and Toitū Te Whenua (Land Information New Zealand).
- Development of a joint data and analytics platform:
  - The Social Wellbeing Agency is developing a data and analytics platform to support the needs of a number of agencies for insights with regards to policy questions that have previously fallen between the gaps.

[84] New Zealand, Statistics New Zealand (Kevin J. Sweeney) (2018), Re-Imagining Data Governance, https://www.data.govt.nz/assets/Uploads/Re-Imagining-Data-Governance_OA.pdf

[85] New Zealand, Government Data Strategy and Roadmap (2021), https://www.data.govt.nz/assets/Uploads/4e-government-data-strategy-and-roadmap.pdf

- Review Data Lab access requirements:
  - The Data Lab controls access to the Integrated Data Infrastructure. They are reviewing access requirements and settings in the hope of expanding access safely.
- Establish the Integrated Data Infrastructure Commons:
  - The Integrated Data Infrastructure Commons will make it easier for Integrated Data Infrastructure users to work together collaboratively, and to share insights from their work with non-users.[86]

Additionally, New Zealand has the Government Enterprise Architecture[87] framework: a layered architecture framework which guides the nation's transformation towards coherent digital government.

Partnership

- New Zealand has Data Practice Communities[88] which ensures partnership and collaboration within certain data ecosystems such as the open data community forums and the Government Analytics Network. Open data community forums are open data discussion forums, websites and meetups where participants can get (and share) information and ideas about the innovative use of open data.
- The Government Analytics Network[89] is a community of practice for government employees working with data. Formed in 2017, it has 300 members from 40 government agencies. It is run by its members with support and guidance from Statistics New Zealand and the Social Investment Agency.
- This Network aims to grow data analytics capability within government organisations by:
  - providing opportunities for learning from others and sharing good practice,
  - linking people and their work to the broader government data analytics community,
  - sharing work updates, reports and conference news,
  - enabling collaboration through regular focus groups.[90]

4. Singapore

Singapore has established a robust data governance framework which consists of various laws, regulations and initiatives aimed at protecting personal data and fostering a trusted environment for data sharing and innovation.

Policies, legislation and regulations

- Legislation and sector-specific regulations can vary, providing different frameworks of rules and restrictions for handling of data in different areas. Regulations include data protection acts, competition acts and sector-specific regulations such as the Banking Act.[91]

[86] Ibid.
[87] New Zealand, Government Enterprise Architecture (2021), https://www.digital.govt.nz/assets/Standards-guidance/Technology-and-architecture/Architecture-Resources/Data-and-information-goverance-and-maturity/Data-and-Information-Governance-Toolkit-Guidelines.pdf
[88] New Zealand, Data practice communities (2023), https://www.data.govt.nz/toolkit/communities-and-groups/
[89] New Zealand, Government analytics network (2023), https://www.data.govt.nz/toolkit/communities-and-groups/government-analytics-network/
[90] Ibid.
[91] Singapore, Infocomm Media Development Authority, Trusted Data Sharing Framework (2019), https://www.imda.gov.sg/how-we-can-help/data-innovation/trusted-data-sharing-framework

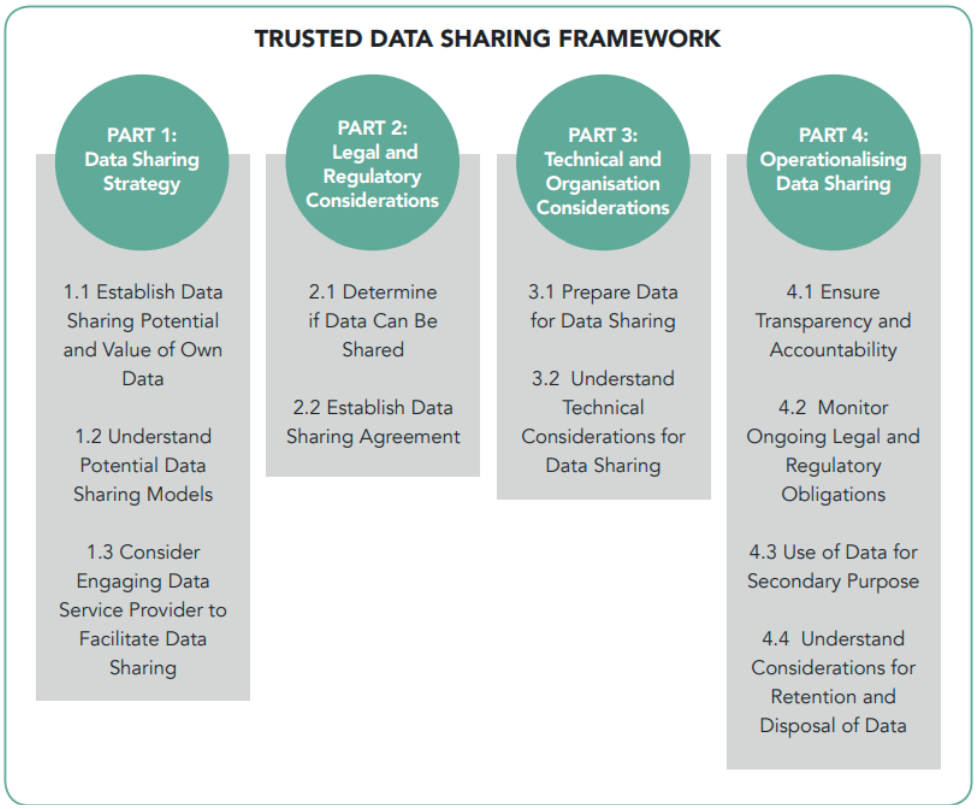
- The Personal Data Protection Act[92] is the primary legislation governing the collection, use and disclosure of personal data in Singapore. It sets out the obligations of organizations in managing personal data and provides individuals with certain rights regarding their personal information.
- The Personal Data Protection Commission[93] is the regulatory body responsible for enforcing the Personal Data Protection Act and promoting compliance with data protection rules. It provides guidance to organizations, conducts investigations and imposes penalties for non-compliance. The Data Protection Advisory Committee has been appointed under this Commission to advise it on matters relating to the review and administration of the personal data protection framework.[94]
- The Data Protection Trustmark is a voluntary certification scheme administered by the Personal Data Protection Commission. It assesses an organization's data protection practices and grants certification to those that meet the required standards and so demonstrate their commitment to data protection.

Institutions, mechanisms and processes

- Singapore's Government Data Office[96] has played a critical role in transforming the data landscape of the country. The new website data.gov.sg, now in public beta, goes beyond being a data repository. It aims to make government data relevant and understandable to the public, through the active use of charts and articles. Data.gov.sg was first launched in 2011 as the government's one-stop portal for publicly available datasets from over 90 government agencies. To date, more than 100 apps have been created using the government's open data.
- The aims of this portal, which is an initiative by the Ministry of Finance and is managed by the Government Technology Agency of Singapore, include seeking to:
  - Provide one-stop access to the government's publicly available data,
  - Communicate government data and analysis through visualisations and articles,
  - Create value by catalysing application development,
  - Facilitate analysis and research.[97]
- Singapore provides technical guidelines for ethical data sharing between organizations via its Trusted Data Sharing Framework[98] released in June 2019. Industry feedback was that the data sharing ecosystem is still in a nascent stage and therefore guidance is required to help organisations, including professional data service providers, overcome concerns connected to data sharing. This Framework aims to guide organisations through their data sharing journey and outlines key considerations for organisations planning data partnerships.

[92] Singapore, Personal Data Protection Act (2012), https://sso.agc.gov.sg/Act/PDPA2012
[93] Singapore, Personal Data Protection Commission, Advisory Committee, https://www.pdpc.gov.sg/Who-We-Are (accessed on 05 July 2023)
[94] Ibid.
[95] Singapore, Personal Data Protection Commission, Data Protection Trustmark, https://www.pdpc.gov.sg/overview-of-pdpa/data-protection/business-owner/data-protection-trustmark (accessed on 05 July 2023)
[96] Singapore, Singapore's national open data collection, https://beta.data.gov.sg/ (accessed on 05 July 2023)
[97] Singapore, Government Developer Portal, Data.gov.sg — The One-Stop Open Data Portal for Publicly Available
[98] Singapore Government Datasets, https://www.developer.tech.gov.sg/products/categories/data-and-apis/data-gov-sg/overview.html (accessed on 05 July 2023)
[98] Singapore, Infocomm Media Development Authority, Trusted Data Sharing Framework (2019), https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf

Figure 9. Singapore's Trusted Data Sharing Framework



Source: Infocomm Media Development Authority[99]

- Singapore's framework introduces six "trust principles": transparency, accessibility, standardisation, fairness and ethics, accountability and security and data integrity.

Some recommended practices are as follows:

- Establishing, documenting, communicating and implementing policies and procedures around data and information and system management, including:
  - Setting up regular meetings amongst stakeholders to monitor data sharing issues.
  - Labelling data assets and objects containing data.
  - Classifying these based on data type, value, sensitivity and importance to the organization.
  - (Where data is highly sensitive) developing a comprehensive data loss prevention strategy, taking into consideration the following specifications:
    - Data at endpoint: data which resides in notebooks, personal computers, portable storage devices and mobile devices,
    - Data in motion: data that traverses a network or that is transported between sites,
    - Data at rest: data in computer storage which includes files stored on servers, databases, backup media and storage platforms.
  - Establishing clearly defined and understood roles and responsibilities across datasets and systems before data is exchanged out of controlled environments.
  - Retaining and destroying data and information.
- Deploying and maintaining policies and procedures around the maintenance of industry-accepted cryptography/encryption protocols for sensitive data in storage (e.g. file servers, databases and end-user workstations), data in use (memory) and data in transmission (e.g. system interfaces, communication over public networks and electronic messaging) as per applicable legal, statutory and regulatory obligations.

[99] Ibid.

- Establishing and maintaining policies and procedures for various types of user access across all systems on the basis of only asking customers for the minimal amount of information necessary.[100]

Technology and infrastructure

- In 2016, the Singaporean government initiated a policy of separating government and public-facing digital services. This led to the need for a bridge or gateway to enable government agencies to securely share data between their internal intranet and the public internet.
- Thus, the Government Data Sharing Platform "API Exchange" (APEX) was launched in 2017. It facilitates data sharing through APIs, enabling secure and seamless access to data across government agencies.
- APEX provides centralized publication, cataloguing, discovery, monitoring and security management for APIs. It plays a crucial role in the "Singpass"[101] public information system, allowing citizens to control the sharing of their personal data.
- There is now an effort to move APEX to the cloud, especially for less-sensitive datasets, and to explore the possibility of creating an API marketplace with the private sector.
- APEX is part of the Singapore Government Technology Stack, a suite of shared and reusable software components and infrastructure maintained by GovTech.[102]

Partnerships

- In November 2019, a private-sector organised Datathon[103] brought together six data contributors from the private and public sectors to test two concepts:
  - That public and private data sharing can take place in accordance with the relevant regulations if a trusted governance framework is in place; and
  - That fusion of public and private datasets can uncover innovative insights, which can in turn drive useful social and potentially commercial outcomes.
- Datathon successfully achieved these outcomes. While the data sharing occurred within a very specific context, participants were then able to share the important lessons they had learned with respect to working with regulators and public and private sector data contributors. This will strengthen further actions to overcome challenges that have traditionally stood in the way of data sharing.[104]

[100] Ibid
[101] Singapore, Singpass, https://www.singpass.gov.sg/main/ (accessed on 05 July 2023)
[102] The World Bank, National Digital Identity and Government Data Sharing in Singapore (2022), https://www.developer.tech.gov.sg/assets/files/GovTech%20World%20Bank%20NDI%20APEX%20report.pdf
[103] Singapore, Infocomm Media Development Authority, Public-Private Data Collaboration Case Study (2019), https://www.imda.gov.sg/-/media/imda/files/programme/data-collaborative-programme/datathon-case-study.pdf
[104] Ibid.

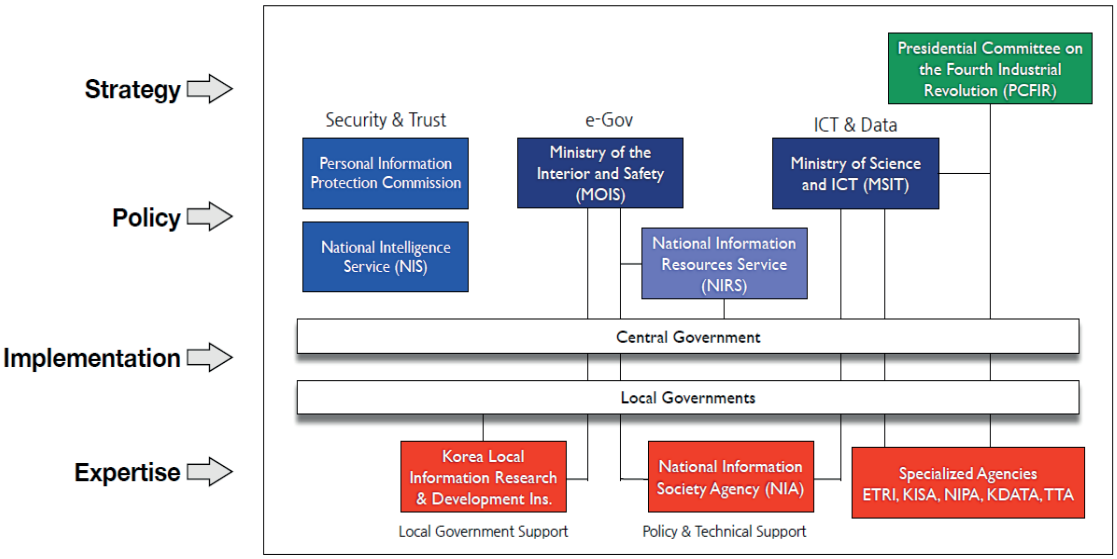
5. Republic of Korea

The Republic of Korea has a comprehensive data governance framework in place to regulate the collection, use and protection of personal data.

Policies, legislation and regulations

- The Republic of Korea's data-related legal framework includes the Framework Act on Intelligent Informatization, the Personal Information Protection Act and the Act on Promotion of the Provision and Use of Public Data. Reflecting a massive paradigm shift powered by AI-driven societal changes, the Framework Act on Intelligent Informatization is a revised version of the Act on Informatization, which had been the legal foundation of the system since 1995.[105]
- The Open Data Law creates a strong legal foundation for the National Information Society Agency, which is responsible for open government data. This law mandates that this Agency support the provision and use of public data.[106]
- The Republic of Korea is focused particularly on how open data can spur a digital transformation and unleash the technologies of the Fourth Industrial Revolution. While Korea's emphasis on and commitment to digital technology is well-known, less attention has been paid to how these efforts could be translated into more extensive cross-organizational interactions, or to how they can enable collaborative forms of governance. In the Republic of Korea's case, the term "public data" is often confused with "open data" because restrictions on private data mean that all open data is open public data.[107]
- Figure 10 shows the Republic of Korea's data governance framework including its strategy and various policy components:

Figure 10: The Republic of Korea's data governance



Source: National Information Society Agency[108]

[105] Carnegie Endowment for International Peace, Data Governance, Asian Alternatives (2022), https://carnegieendowment.org/files/Data_Governance_v1.pdf

[106] UNESCAP, Open Government Data Policies and Practices in the Republic of Korea (2020), https://www.unapcict.org/sites/default/files/2020-07/Open%20data%20policies%20and%20practices%20in%20the%20ROK_FINAL.pdf

[107] Carnegie Endowment for International Peace, Data Governance, Asian Alternatives (2022), https://carnegieendowment.org/files/Data_Governance_v1.pdf

[108] National Information Society Agency (Jong-Sung Hwang, Ph.D), Korea's Data Ecosystem (2022), https://www.worldbank.org/content/dam/infographics/780xany/2022/apr/Presentations/Korea-s-DataEcosystem-20220428.pdf

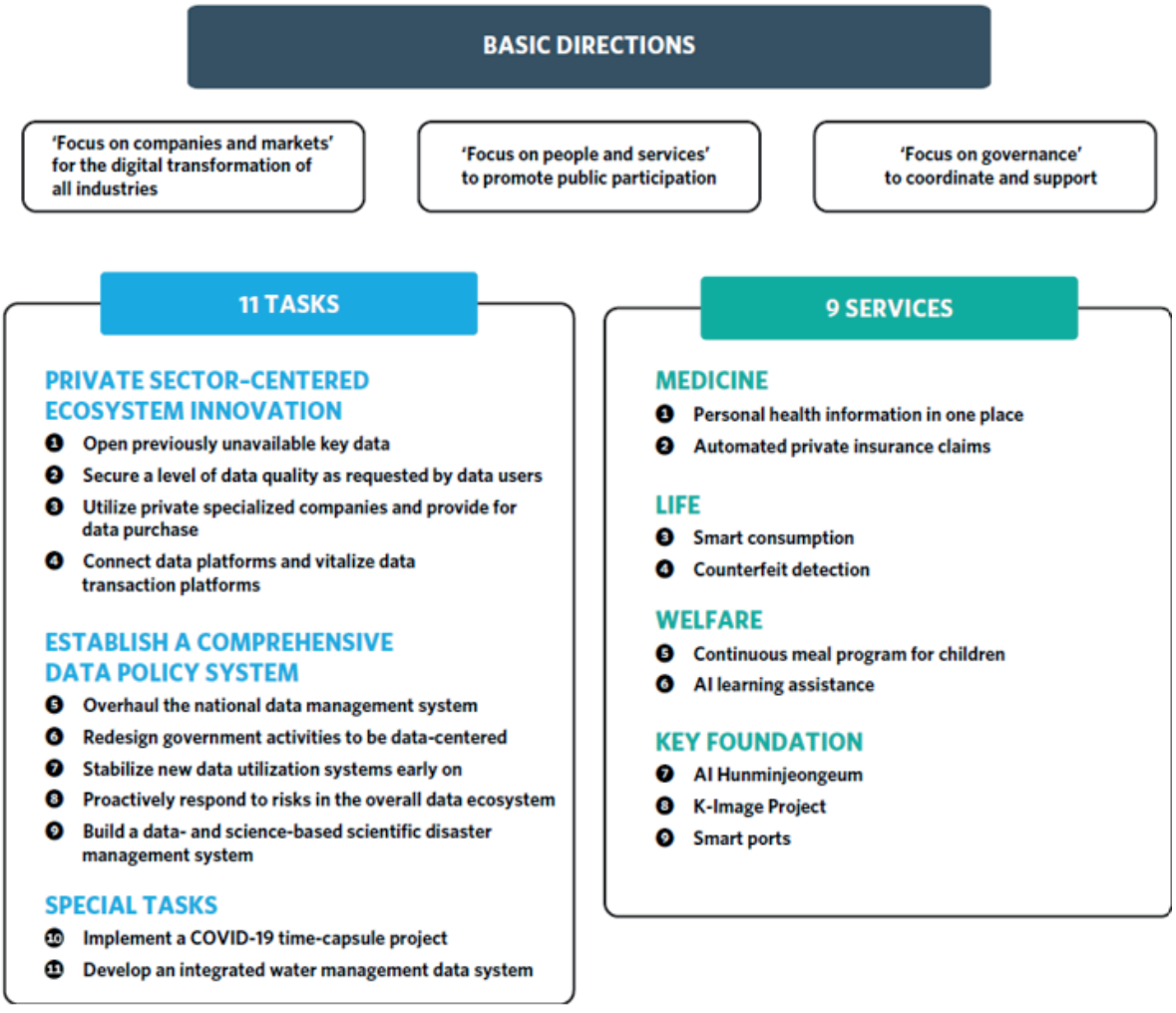
Institutions, mechanisms and processes

- An important initial consideration for understanding the Republic of Korea's open data policies is the country's institutional underpinnings. The Ministry of the Interior and Safety, the Ministry of Science and Information and Communications Technology and Statistics Korea each oversee some aspects of the Republic of Korea's open data policies. These three central agencies play different roles: overseeing public-sector data, private-sector data and authorized statistical data respectively.
  - The Republic of Korea's bureaucratic diversity has been replicated in laws and regulations. For instance, the Ministry of Science and Information and Communications Technology is responsible for implementing the Framework Act on Intelligent Informatization, but the Ministry of the Interior and Safety is responsible for implementing the Act on Promotion of the Provision and Use of Public Data. This regulatory diversity, in turn, has created confusion. And no one law specifies which government body or bodies have the jurisdiction to manage some of the data that the private sector generates.
  - The same is true when local governments become involved. For instance, the Republic of Korea's current law on informatization requires all provincial and local governments to submit basic plans for informatization (including open data) to the head of the Ministry of the Interior and Safety as this official formally has responsibility for local government. But they must then provide these local plans to the Minister of Science and Information and Communications Technology as it is they who have thematic oversight.
  - As a result, these two ministers need to coordinate and collaborate. This can be difficult, however, because public data (under the Ministry of the Interior and Safety) cannot be easily integrated with private data (under the Ministry of Science and Information and Communications Technology). The two different ministries' jurisdictions may functionally overlap but they remain institutionally divided.
  - The Republic of Korea's institutions will need to evolve to combine data from many different types of organizations. And these institutional frictions are mirrored in contradictory legal and regulatory provisions and a lack of consensus among wider public and private stakeholders.
- In addition, the differences between the kinds of data these three agencies oversee are not entirely clear-cut. Since 2021, the MyData project in the Republic of Korea has allowed accredited companies to manage personal information scattered across the financial, telecommunications, medical and public sectors. This project enables the further use of data through the pseudonymization and anonymization of personal information. In this sense, the distinction between big data in the private sector and existing open public data is becoming less pronounced, but as open data has in the past always meant public data the jurisdictional boundaries among the Republic of Korea's three major regulatory and policy institutions are also growing blurred.
- Other government agencies also shape policies that affect open data initiatives at the national level. For example, the Personal Information Protection Commission is a powerful regulator in charge of data security and privacy protection. This commission enforces privacy protection legislation and so is empowered to step in when any of the three lead agencies involved with open data threaten to harm citizens' privacy.
- Meanwhile, the Presidential Committee on the Fourth Industrial Revolution designs and coordinates the Republic of Korea's national digital policies. This committee has a "Data Special Subcommittee," which consists of experts and practitioners from related ministries, industries and academia. Additionally, the Republic of Korea Data Project, which strives to harvest and harness ideas from the private sector, seeks to promote the opening, distribution and utilization of data. And these are not the only relevant initiatives: Figure 11 shows eleven tasks and nine services conducted by a specific ministry or through collaboration between ministries. The three key institutions play especially important roles in all eleven tasks but are

by no means the only stakeholders or implementers.

- In terms of top-level leadership, the Open Data Strategy Council, which is co-chaired by the Prime Minister and a data expert from the private sector, designs the basic plans for opening public data and improves these plans to assure better usage of public data. This council is a deliberative body that examines, coordinates, monitors and evaluates government decisions and the implementation of major open data policies and plans. The Ministry of the Interior and Safety then formulates and refines the open data master plan, evaluates implementation, creates the relevant infrastructure, and releases data. Participating organizations under the council play other specific roles. To cite a few examples: the Open Data Center for Policy and Technical Support provides technical assistance and acts as a hub and clearinghouse for open data, the Chief Open Data Officer leads open data efforts at all public organizations and the Open Data Mediation Committee handles decisions to stop data sharing and disputes over public organizations' refusal to share data.

Figure 11. The Republic of Korea's approach to data-driven innovation



Source: Carnegie Endowment for International Peace[109]

[109] Carnegie Endowment for International Peace, Data Governance, Asian Alternatives (2022), https://carnegieendowment.org/files/Data_Governance_v1.pdf

- Clearly, the Republic of Korea lacks a unitary national institution for data management and control, which, in turn, makes it difficult to move and share data across sectors, domains and organizational boundaries. To remedy this problem, the Republic of Korea has considered establishing a new ministry-level data agency, but the performance of any such agency would invariably depend on the attitude (and cooperation) of other existing ministries. A particular issue where a mutually satisfactory solution has not yet been found is the question of who should manage the relationships between ministries managing open data.[110]

6. Switzerland

Switzerland has a strong data governance framework in place to regulate the collection, processing and protection of personal data.

Policies, legislation and regulations

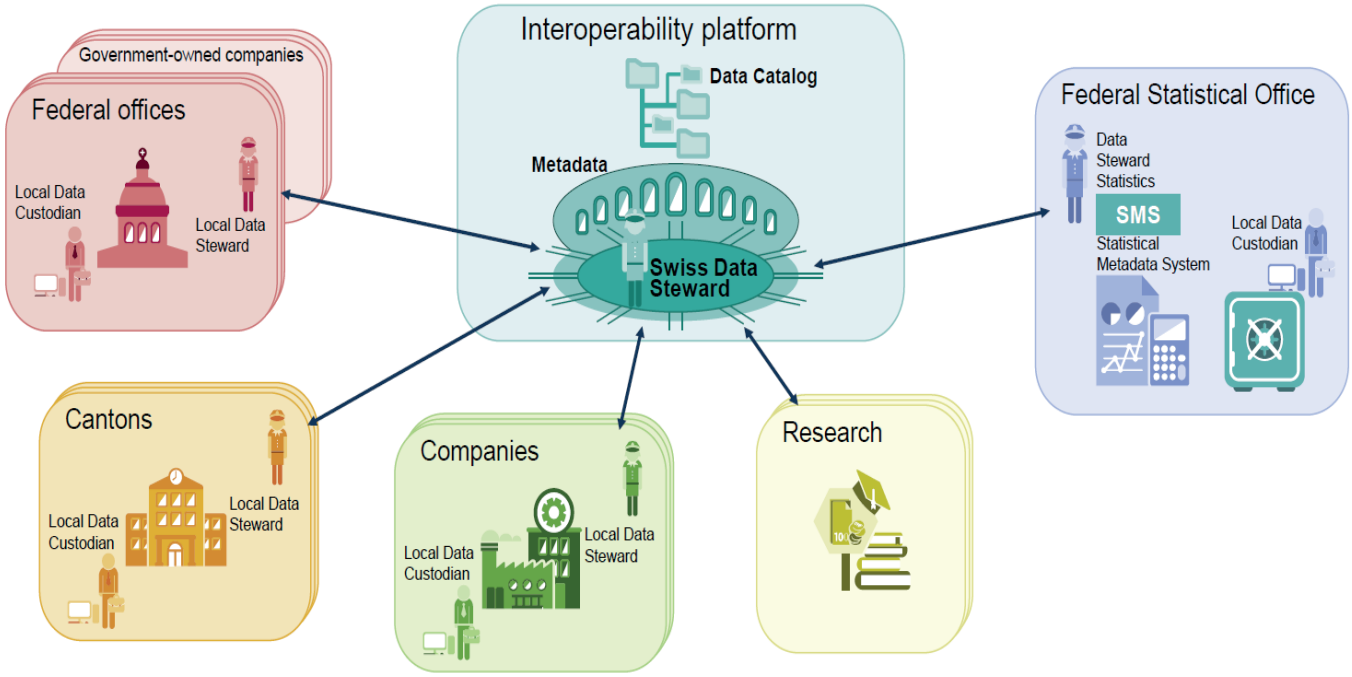
- Switzerland has a comprehensive legal framework for data governance, including the Federal Act on Data Protection. It regulates the processing of personal data and provides guidelines for data protection and privacy.
- Switzerland has introduced a new Federal Act on Data Protection[111] to enhance data protection and rights for Swiss citizens. This legislation became mandatory for Swiss companies to comply with on September 1, 2023. The new Act addresses the need for comprehensive data protection regulations in the context of advancing technology and societal changes.
- Key changes introduced by the new Act for businesses include:
  - Coverage: The new act covers the data of natural persons, not just legal entities.
  - Sensitive Data: Genetic and biometric data are now categorized as sensitive data.
  - Privacy Principles: “Privacy by Design” and “Privacy by Default” principles are introduced. The principle of Privacy by Design requires incorporating data protection into the structure of products or services that collect personal data. Privacy by Default ensures high-level security is the default setting for data protection.
  - Register of Processing Activities: Keeping a register of data processing activities becomes mandatory, with exemptions for small and medium-sized enterprises where data risk is low.
  - Data Breach Notification: Prompt reporting of data security breaches to the Federal Data Protection and Information Commissioner is now required.
  - Profiling: The automated processing of personal data, known as profiling, is now regulated by law.
- These changes aim to align Swiss data protection laws with evolving technology and social developments while ensuring data compatibility with EU regulations to maintain the free flow of data with the EU.[112]

[110] Ibid.
[111] Switzerland, Federal Council, New Federal Act on Data Protection, https://www.kmu.admin.ch/kmu/en/home/facts-and-trends/digitization/data-protection/new-federal-act-on-data-protection-nfadp.html (accessed on 07 July 2023)
[112] Ibid

Institutions, mechanisms and processes

- The Federal Data Protection and Information Commissioner [113] oversees data protection in Switzerland and provides guidance on data governance practices.
- The Swiss Federal Council, which is the nation's executive body, establishes policies and regulations related to data governance.
- The role of the Federal Statistical Office is changing from that of a classical statistical office to an institute for data management suitable to play a substantial role in a broad-based data ecosystem. The key concept is to keep data storage and ownership decentralised in individual administrative and statistical units but to make the data available and re-usable by sharing it with other units.
- Interoperability of data is a key pillar for introducing the "once-only" principle for data collection and re-use.
- Another key feature of the new system is the creation of a centre of expertise for data science at the Federal Statistical Office. This centre will benefit the whole of the Federal Administration by offering data innovation services to all.
- The Swiss Data Steward is centrally located in the Swiss Federal Statistical Office and is responsible for:
  - Coordinating the standardization and harmonization process.
  - Identifying and describing the data requirements of the various users.
  - Managing the content of metadata (data catalogue).
  - Validating the quality assurance of metadata and data in the administrative areas using data analyses.

Figure 12. Swiss Data Stewardship



Source: Swiss Federal Statistical Office[114]

[113] Switzerland, Federal Data Protection and Information Commissioner, https://www.edoeb.admin.ch/edoeb/en/home.html (accessed on 07 July 2023)

[114] Switzerland, Swiss Federal Statistical Office, National Data Management NaDB (2020), https://unece.org/fileadmin/DAM/stats/documents/ece/ces/2020/S8_Switzerland.pdf

- A National Data Management programme was launched in October 2019 under the responsibility of the Federal Statistical Office.
- To promote the re-use of data in the long term, a metadata catalogue has been prepared containing descriptions and information about shared data. An interoperability platform has been developed and is available to all participating offices.
- The current steps anticipate the implementation of several projects within specified areas (wages, occupational profiles, taxes, health provision). Drawing on previous experience, the project will consider whether the procedure is compatible with the long-term implementation of the once-only principle and shall be adapted if necessary. Data protection and privacy considerations, as well as necessary amendments to legal frameworks, will be part of the program.
- Individual offices will not have to build up their own expertise in this complex and volatile area, but instead will be able to buy in the services of the Federal Statistical Office's Competence Centre for Data Science. With its wealth of experience in data quality and the various methods of data processing, the Federal Statistical Office is the natural choice to host this centre.[115]
- The opendata.swiss portal is a central and reliable platform enabling simple access to open government data in Switzerland. The platform also references data from third parties – state-related enterprises, persons who perform tasks for the Confederation, cantons and communes – where there is a public interest in such data, even if they are already referenced on other websites. By referencing data in this centralised manner, the portal plays a fundamental role in data infrastructure and creates an environment encouraging the use of data. The portal only points users to data sources, the published data continues to be held by the individual data owners, thus avoiding data redundancy. As far as possible, the portal operator ensures that the metadata of data already published elsewhere are automatically incorporated into that dataset's listing on opendata.swiss.[116]

7. United Kingdom

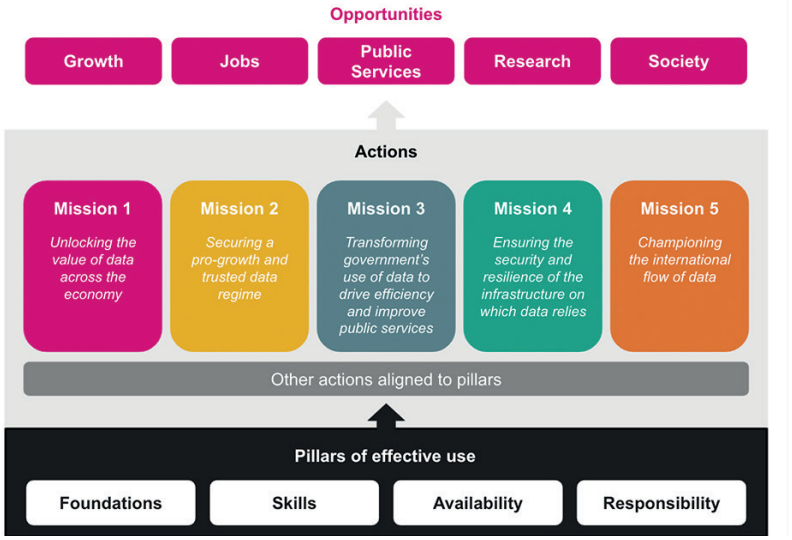
The UK has a comprehensive data governance framework that encompasses various laws, regulations, guidelines and institutions to govern the management, protection and use of data.

Policies, legislation and regulations

- The primary legislation governing data protection in the UK is the Data Protection Act 2018. The Data Protection Act supplements the GDPR. The Act is a complete data protection system, so as well as governing the processing of personal data covered by the GDPR, it also covers all other processing of personal data for UK law enforcement and national security. It makes a number of agreed modifications to the GDPR to make it work for the benefit of the UK in areas such as academic research, financial services and child protection.[117] The UK government promotes data sharing and open data initiatives to foster transparency and innovation.[118]
- The UK has a National Data Strategy.[119] A theory of change can be found within it:

[115] Ibid.
[116] Switzerland, Swiss Federal Statistical Office (2021), Strategy for open government data in Switzerland 2019 - 2023 https://www.bfs.admin.ch/bfs/en/home/services/ogd/documentation.assetdetail.16164831.html
[117] United Kingdom, Department for Digital, Culture, Media & Sport (2020), National Data Strategy, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy
[118] United Kingdom, Digital Economy Act (2017), https://www.legislation.gov.uk/ukpga/2017/30/contents/enacted
[119] United Kingdom, Department for Digital, Culture, Media & Sport (2020), National Data Strategy, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy

Figure 13. UK's Data Strategy



Source: UK Department for Digital, Culture, Media & Sport[120]

- The UK has also prepared a Data Sharing Governance Framework:
  - This Framework provides principles and actions to reduce or remove common non-technical frictions and barriers, now and over time. It highlights the relationship between technical data standards and wider data governance.
  - Applying the principles and actions in this Framework will set departments and public bodies on a course to greater alignment of data sharing systems and processes, and embed data sharing as a strategic priority across government.
  - The publication of the Framework supports commitments made in the National Data Strategy, particularly in addressing barriers to data sharing and driving aligned data governance structures across government. The Framework also supports the Declaration on Government Reform, which commits to openness and data sharing across government.
  - This Framework is one of a growing suite of tools which enable better use, reuse and sharing of data across government, including the Government Data Quality Framework and the Data Ethics Framework[121].

Institutions, mechanisms and processes

- The UK has a Central Digital and Data Office and a Chief Data Officer. The Central Digital and Data Office is part of the Cabinet Office. They lead on the digital, data and technology functions of government.
- The Department for Digital, Culture, Media and Sport is leading the work on implementing the National Data Strategy's commitments with respect to data sharing in the wider economy and will provide separate guidance on interventions to maximise value for money and impact in that context.[122]
- The Information Commissioner's Office[123] is an independent authority in the UK responsible for promoting and enforcing data protection laws. It provides guidance to organizations,investigates data breaches and imposes penalties for non-compliance. The Office's role is crucial in ensuring that organizations handle personal data in a lawful and responsible manner.[124]

[120] Ibid.
[121] United Kingdom, Central Digital and Data Office, Data Sharing Governance Framework (2022), https://www.gov.uk/government/publications/data-sharing-governance-framework/data-sharing-governance-framework
[122] Ibid.
[123] United Kingdom, Information Commissioner's Office, ICO25 strategic plan, https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/ico25-plan/ (accessed on 21 June 2023)
[124] Ibid.

- The UK government also operates data.gov.uk[125], a portal that provides access to a wide range of open datasets from various government departments and public sector organizations.
- The Centre for Data Ethics and Innovation[126] is an independent advisory body that provides recommendations on the ethical use of data and emerging technologies. It conducts research, advises policymakers and promotes public dialogue to ensure that data-driven technologies are developed and deployed in a fair and ethical manner.
- The UK has specific data governance frameworks for information governance in healthcare.[127]

Technology and infrastructure

- The Data Standards Authority[128] was established in April 2020 as a multi-disciplinary team drawn from a variety of data-related backgrounds in technology, strategy and policy. It works to improve the public sector's management of data.
  - It does this by establishing standards to make it easier and more effective to share and use data across government.
  - Working with experts across the wider public sector and devolved administrations, the private sector and academia, the Data Standards Authority identifies, improves and helps implement data standards that meet user needs.
  - The Authority recommends a number of standards, guidance and other resources the departments can follow when working on data projects.
- The GOV.UK Service Standard[129] assists teams in creating and running public services. When working on data projects, the Data Standards Authority recommends service manual guidance from this standard to help users to:
  - improve metadata sharing[130] across government,
  - choose data tools and infrastructure that are flexible, scalable, sustainable and secure.
- The Technology Code of Practice[131] is a set of cross-government criteria to help design, build and buy technology. When planning data projects, the Data Standards Authority recommends the stakeholders pay particular attention to certain parts of the Technology Code of Practice, which they can use to:
  - make use of open data standards[132] to build technology that is easier to expand, upgrade and use with other technologies,
  - plan and design projects that meet data security requirements,[133]
  - make better use of data by improving stakeholder technology, infrastructure and processes, and[134]
  - manage stakeholder data for access, reuse and independent maintenance outside of the context of specific technologies or services.[135]

[125] United Kingdom, Find open data, https://www.data.gov.uk/ (accessed on 21 June 2023)
[126] United Kingdom, Centre for Data Ethics and Innovation, https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation (accessed on 27 June 2023)
[127] United Kingdom, NHS England, https://www.england.nhs.uk/ig/about/ (accessed on 27 June 2023) [128] United Kingdom, Data Standards Authority, https://www.gov.uk/government/groups/data-standards-authority (accessed on 27 June 2023)
[129] United Kingdom, Service manual, https://www.gov.uk/service-manual/service-standard (accessed on 27 June 2023)
[130] United Kingdom, Metadata standards for sharing and publishing data, https://www.gov.uk/government/collections/metadata-standards-for-sharing-and-publishing-data (accessed on 30 August 2023)
[131] United Kingdom. The Technology Code of Practice, https://www.gov.uk/guidance/the-technology-code-of-practice (accessed on 29 June 2023)
[132] United Kingdom, Guidance, Make use of open standards, https://www.gov.uk/guidance/make-use-of-open-standards (accessed on 29 June 2023)
[133] United Kingdom, Guidance, Make things secure, https://www.gov.uk/guidance/make-things-secure (accessed on 29 June 2023)
[134] United Kingdom, Guidance, Make better use of data, https://www.gov.uk/guidance/make-better-use-of-data (accessed on 29 June 2023)
[135] United Kingdom, Guidance, Manage your data for access and reuse, https://www.gov.uk/guidance/manage-your-data-for-access-and-reuse (accessed on 30 June 2023)

- UK guidelines state that the use of APIs can be core to starting and developing data projects. Stakeholders following these guidelines can:
  - design, build and run APIs to deliver the best service to users,[136]
  - discover APIs in the government API Catalogue[137] to increase the reuse of data and reduce the duplication of effort in data projects, and
  - meet API technical and data standards[138] to help deliver better services.

Partnership

- The UK government collaborates with various stakeholders, including regulators, industry bodies and academic institutions, to develop and maintain the data governance framework. This includes partnerships with organizations such as the Open Data Institute and the Alan Turing Institute, who focus on promoting data openness, data ethics and data-driven innovation.[139]

8. United States of America

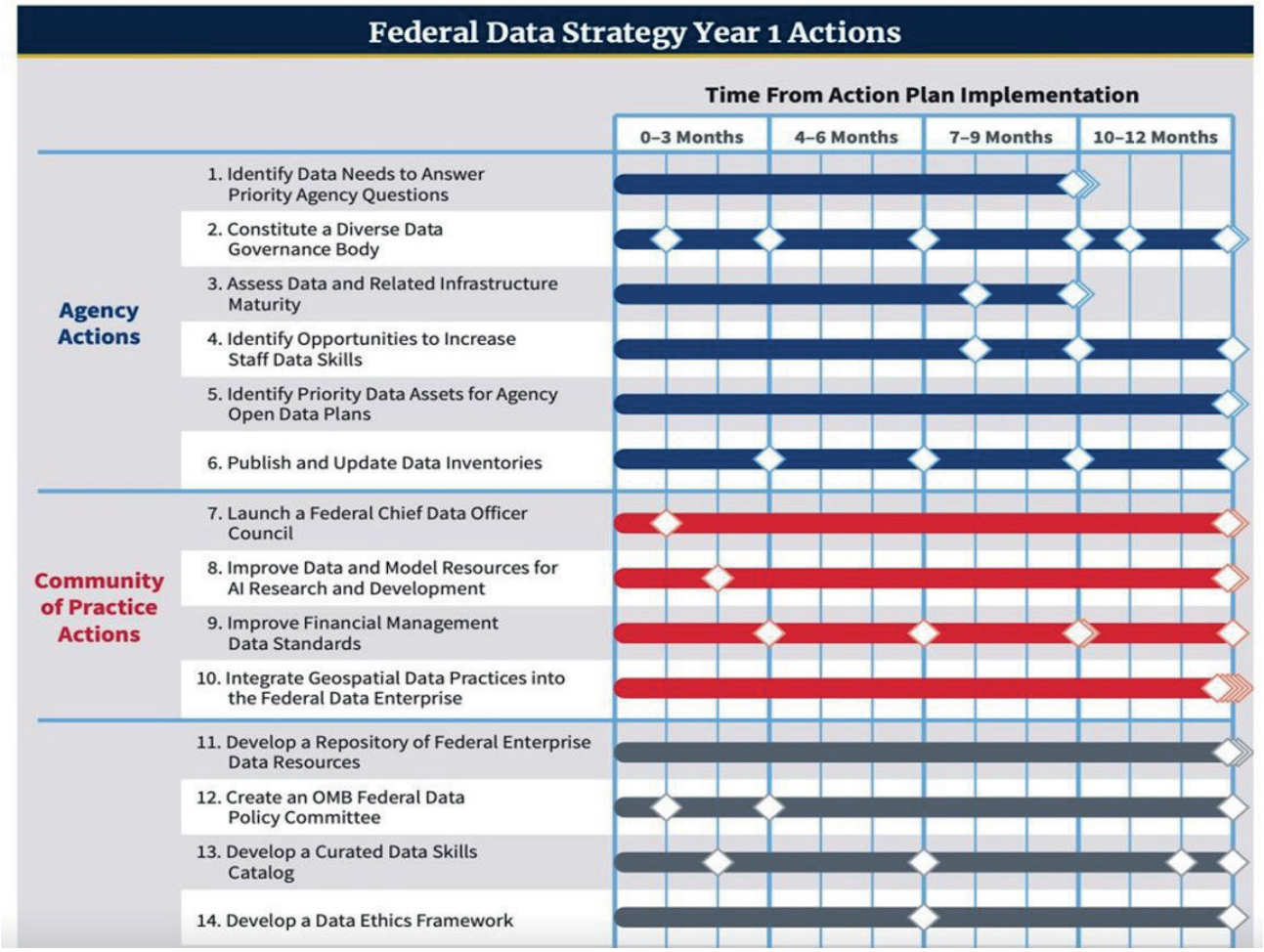
The data governance framework in the USA involves a combination of policies, regulations, institutional mechanisms, skilled professionals, technological infrastructure and partnerships to ensure the effective management, protection and responsible use of data across various domains and sectors.

Policies, legislation and regulations

- In June 2019, the USA's government introduced the Federal Data Strategy, a ten-year vision for optimizing federal data assets while maintaining security, privacy and confidentiality. The strategy is built upon three core principles: ethical governance, conscious design and a learning culture.
- The USA has a history of various initiatives, policies, executive orders and laws that have positioned it as a leader in government data management and reuse.
- The Federal Data Strategy outlines 40 practices to guide agencies in adopting the strategy, emphasizing the connection between user needs and effective data resource management.
- Federal agencies are required to follow annual government action plans to ensure consistent implementation of the strategy. These action plans include prioritized steps, timeframes, and responsible entities.
- A draft version of the 2019-2020 Federal Data Strategy Action Plan encompasses 16 critical steps for launching the initial phase of the data strategy. These steps include developing data ethics frameworks and providing data science training for federal employees.[140]
- An example of a public sector institution's annual action plan is included in the USA Government's Federal Data Strategy:

[136] United Kingdom, API design guidance, https://www.gov.uk/government/collections/api-design-guidance (accessed on 01 July 2023)
[137] United Kingdom, UK public sector APIs, https://www.api.gov.uk/#uk-government-apis (accessed on 01 July 2023)
[138] United Kingdom, Guidance, API technical and data standards, https://www.gov.uk/guidance/gds-api-technical-and-data-standards (accessed on 01 July 2023)
[139] United Kingdom, Department for Digital, Culture, Media & Sport, National Data Strategy (2020), https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy
[140] OECD, The Path to Becoming a Data-Driven Public Sector (2019), https://www.oecd-ilibrary.org/sites/9cada708-en/index.html?itemId=/content/component/9cada708-en#endnotea2z34

Figure 14: USA Government's Federal Data Strategy



Source: The US Government Federal Data Strategy[141]

- The USA has several sector-specific laws and regulations. Examples include:
  - Driver's Privacy Protection Act for motor vehicle information.
  - Children's Online Privacy Protection Act for children's online data.
  - Video Privacy Protection Act for video and audio-visual material rental records.
  - Cable Communications Policy Act for subscriber privacy in cable services.
- Various states have enacted data breach notification laws that affect businesses regardless of their physical presence in that state, often with respect to the unauthorized access to personal information. For example, California introduced the California Consumer Privacy Act in 2018, enhancing consumer rights and business obligations. States such as Virginia, Colorado, Utah, Connecticut, Iowa, Indiana, Montana and Tennessee have also passed comprehensive data privacy laws.
- The Federal Trade Commission plays a significant role in shaping federal privacy and data security policy.[142]
- The National Institute of Standards and Technology has released a special publication on "De-Identifying Government Datasets: Techniques and Governance"[143] with the co-authorship of the US Census Bureau in September 2023.

[141] United States of America, The US Government Federal Data Strategy (2020), https://strategy.data.gov/assets/docs/2020-federal-data-strategy-framework.pdfInstitutions, mechanisms and processes

[142] F. P. Pittman, A. Hafiz, A. Hamm, White & Case LLP, ICLG.com, Data Protection Laws and Regulations USA 2023, https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa (accessed on 12 July 2023)

[143] United States of America, National Institute of Standards and Technology (2023), https://csrc.nist.gov/pubs/sp/800/188/final

Institutions, mechanisms and processes

- Various federal agencies, such as the Office of Management and Budget, the National Institute of Standards and Technology and the Federal Trade Commission contribute to data governance through the development of policies, guidelines and frameworks.
- As part of the Federal Data Strategy, the Office of Management and Budget (OMB) was set to create a Data Council within the White House by November 2019. This council coordinates the strategy and influences budget priorities related to data management and utilization.
- The Open, Public, Electronic, and Necessary Government Data Act defines the role and responsibilities of a Chief Data Officer within federal agencies. These responsibilities include:
  - Managing the entirety of data's lifecycle.
  - Coordinating with other officials within the agency responsible for data to meet the agency's data needs.
  - Managing agency data assets, including standardizing data formats, sharing data assets and publishing data assets in accordance with the law.
  - Ensuring agency data conforms to best practices.
  - Engaging agency employees, the public and contractors to improve data use through collaboration.
  - Supporting performance improvement and evaluation officers in using data for their respective functions.
  - Reviewing the impact of agency infrastructure on data accessibility and working with the Chief Information Officer to enhance data accessibility.
  - Maximizing the use of data within an agency for various purposes, including evidence production, cybersecurity and operational improvement.
  - Identifying points of contact for open data-related roles and responsibilities.
  - Serving as the liaison to other agencies and the OMB on optimizing existing agency data for statistical purposes.
  - Ensuring compliance with regulations and guidance related to data management, including required certification and training[144].

9. Other country examples

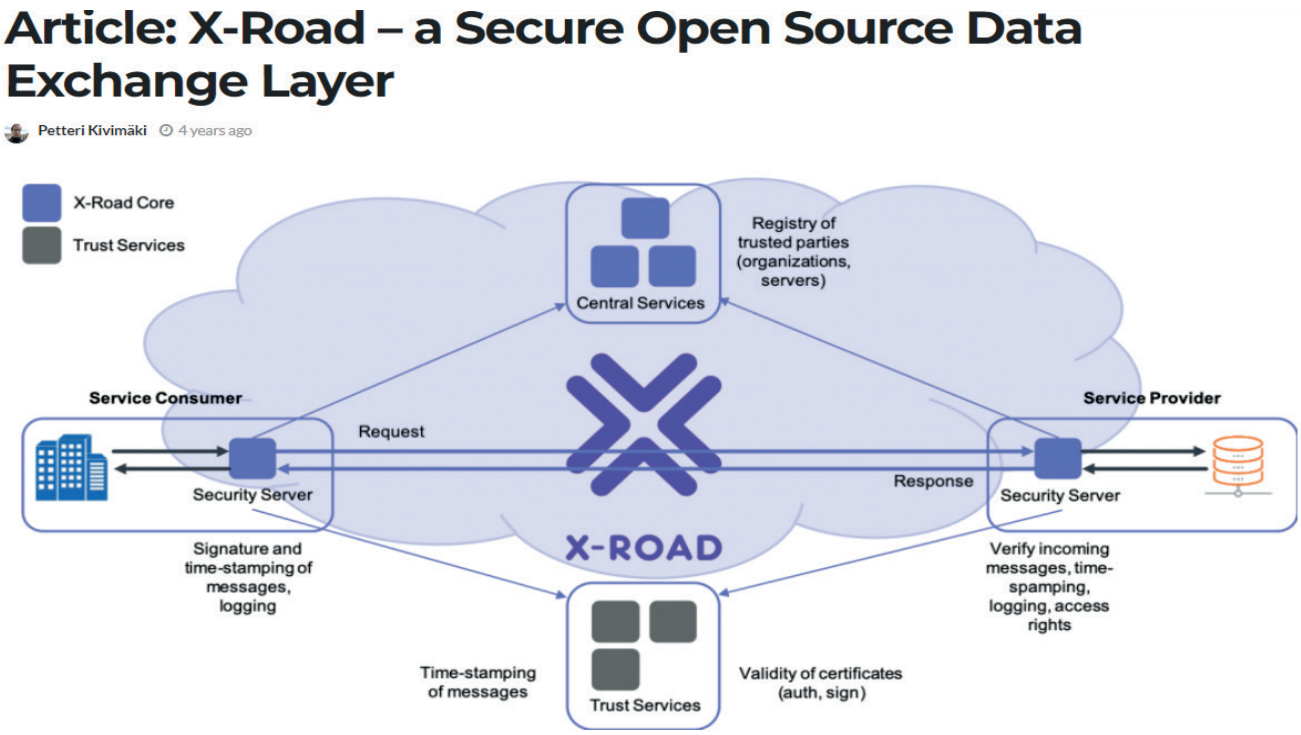
Another example of the use of technology and infrastructure in data governance is X-Road which Finland, Estonia and Iceland have been using for open-source data exchange[145].

The identity of each organization and its technical entry point (the security server) is verified using certificates. These are issued by a trusted certification authority when an organization joins an X-Road ecosystem. These identities are maintained centrally, but all the data is exchanged directly between organizations. The routing of data is organised by X-Road, which maps the identifying information it holds onto the physical network locations of the services. An authenticated electronic paper trail regarding the data exchange is stored locally by the data exchange parties, and no third parties have access to the data. Time-stamping and digital signatures together undeniably authenticate that data sent via X-Road did indeed arrive (this is known as data nonrepudiation):

[144] OECD, The Path to Becoming a Data-Driven Public Sector (2019), https://www.oecd-ilibrary.org/sites/9cada708-en/index.html?itemId=/content/component/9cada708-en#endnotea2z34

[145] Giulia Guadagnoli, A conversation with Petteri Kivimäki on X-Road, Open Source Observatory (2021), https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/open-source-international-cooperation

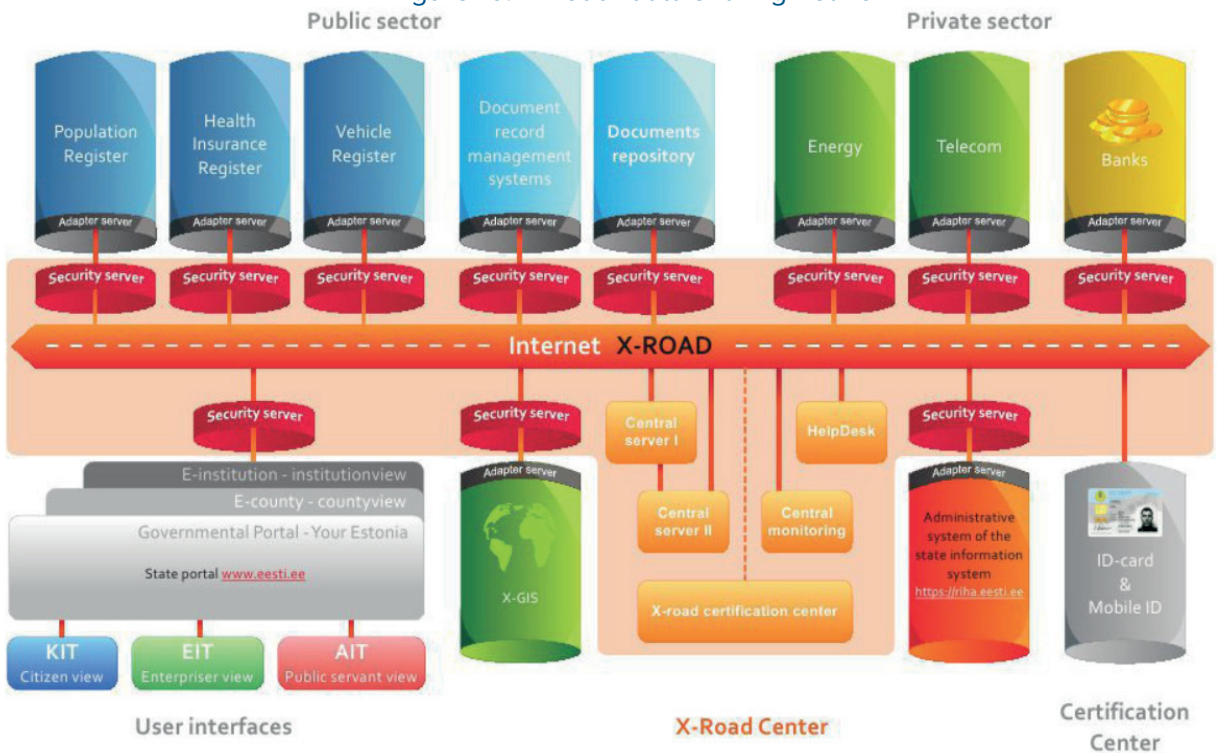
Figure 15. X-Road: a secure open-source data exchange layer



Source: Kivimäki [146]

Another illustration of the X-Road included in Figure 16:

Figure 16. X-Road- data sharing network



Source: UK Government Digital Service Blog[147]

[146] Petteri Kivimäki, Article: X-Road – a Secure Open Source Data Exchange Layer (2019), https://www.apiscene.io/lifecycle/article-x-road-a-secure-open-source-data-exchange-layer/

[147] UK Government Digital Service Blog, 'Government as a data model': what I learned in Estonia (2013), https://gds.blog.gov.uk/2013/10/31/government-as-a-data-model-what-i-learned-in-estonia/

D. Recommended data governance framework for Türkiye

1. Purpose, principles and recommendations

A solid and inclusive data governance framework is an indispensable tool in Türkiye's digital transformation. With the adoption of international standards and frameworks, active engagement of stakeholders and use of new technologies and data sources, Türkiye is poised to unlock the full potential of data, leading to better policies, better run public services and an accelerated digital transformation. This report provides key recommendations from UNDP for Türkiye's data governance framework with regards to the principles, pillars and main action points UNDP suggests would be useful to include. It aims to provide strategic insights and a contextual understanding, rather than itself serving as a comprehensive set of guidelines.

The recommended principles represent the Government of Türkiye's core values with respect to data. This will form the strategic foundation of the suggested approach. The data governance framework needs to be grounded in human rights based ethical principles. These outline how to leverage data collaboratively and responsibly, while demonstrating transparency, stewardship and excellence, as articulated by the Guidance Note prepared by UN OHCHR.[148]

In this context, UNDP proposes a data governance framework grounded in the following principles:

- Protect human rights: The core principle of data governance is to place human rights at the forefront. As digital technology continues to evolve, so does our awareness of its impact on human rights, both positive and negative. Utilizing data should involve both harnessing its potential for the betterment of humanity and ensuring that it is managed responsibly by maintaining a strong focus on safeguarding human rights.
- Inclusive approach: To ensure effective data governance, an inclusive approach must be guaranteed, where all processes revolve around the needs of all people. Building an inclusive data ecosystem empowers individuals and contributes to the creation of an accessible society. Therefore, data governance should cater to the requirements of all stakeholder groups, and involve their input in all phases of data collection activities.
- Maintain ethical standards: Data ethics encompasses the moral considerations related to data management, covering everything from data generation and recording to collection, usage and sharing. It is of heightened importance when data activities have the potential to significantly impact individuals and society, directly or indirectly. To ensure robust data governance, the highest ethical standards must be maintained throughout the data lifecycle.
- Empower people through data: A key aspect of data governance involves enhancing data literacy skills within organizations and among external partners. This empowerment enables individuals to effectively work with data, fostering a culture of data-driven decision-making and problem-solving.
- Accountability: Accountability, from a human rights perspective, implies that those in authority, whether the State or other actors, must answer for their decisions and actions to the affected population. This aligns with international human rights law, where duty-bearers (those in authority) are accountable to rights-holders (the affected population).
- Promote transparency: Transparency and the provision of information to the public are paramount in data governance. Data collectors should provide clear and openly accessible information about their operations, including with respect to research design and the data collection methods they use. State agencies should make the data they collect openly accessible to the public. This aligns with the public's right to information.

[148] UN Human Rights Office of the High Commissioner (OHCHR), Human Rights-Based Approach to Data (HRBAD) (2018), https://www.ohchr.org/sites/default/files/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf

- Promote a culture of data innovation, learning and sharing: Data governance should encourage open digital standards and open data practices, fostering reusability and interoperability. Digital public goods can unlock transformative solutions and digital infrastructures, creating a more equitable and transparent future while protecting rights and preventing misuse. Additionally, a culture of data innovation, continuous learning and expertise sharing supports data-driven decision-making and democratic governance, particularly by inviting wider citizen participation in decision-making processes.

The recommended data governance framework for Türkiye encompasses five pillars, listed below and indicated in Figure 17:

1. Policies, legislation and regulations: Focusing on Türkiye's readiness to comply with international data legislation/regulations.
2. Institutions, mechanisms and processes: Analysing institutional mechanisms and identifying key actors.
3. People: Building capacity within government institutions, the private sector, academia and civil society organizations to enable responsible data practices.
4. Technology and infrastructure: Assessing the technical components of data processing and identifying technologies required for data flow, interoperability and security.
5. Partnerships: Encouraging collaboration and partnerships among stakeholders to facilitate data exchange and collective efforts.

Figure 17. Data policy recommendation: Türkiye's data governance framework

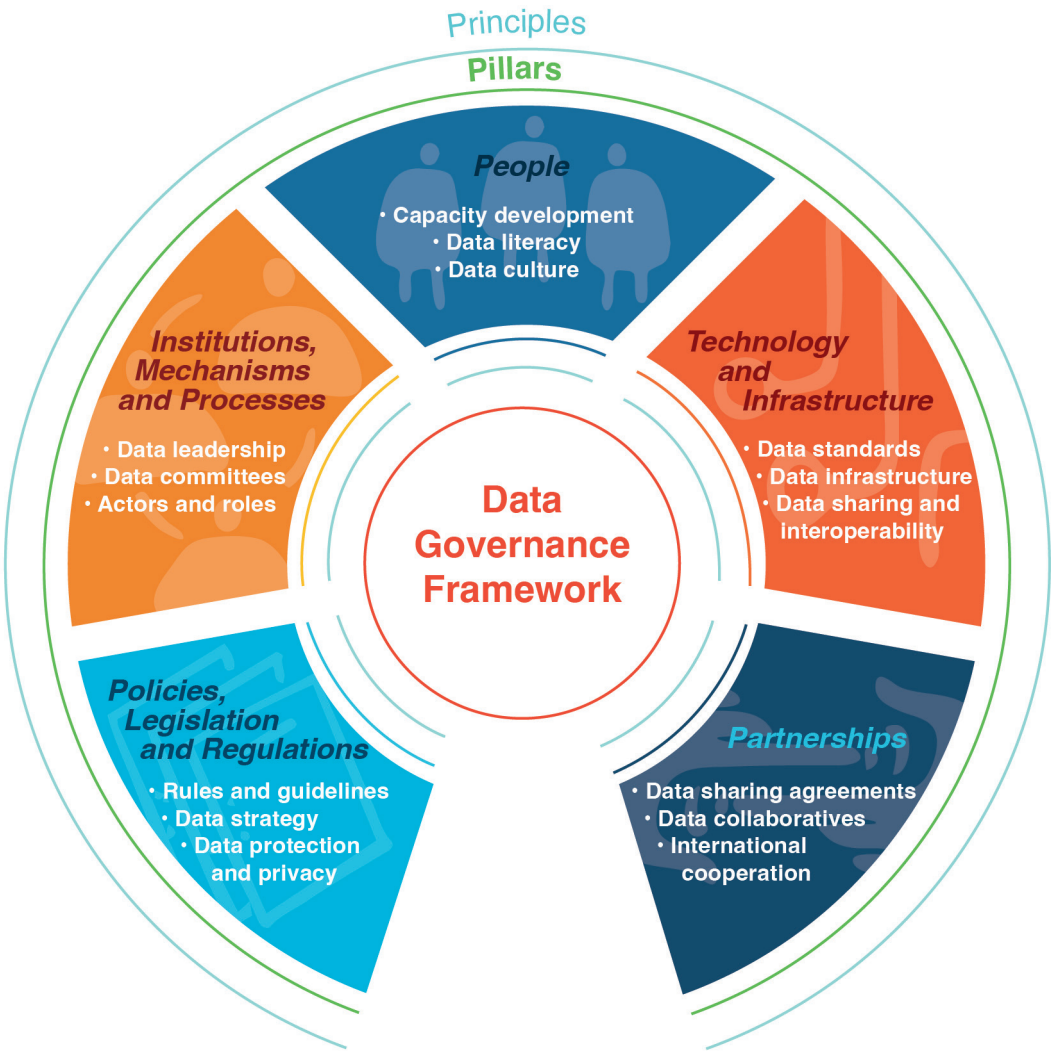


Figure 18 shows the recommendations for the data governance framework under each pillar. Detailed suggestions and further information with respect to each of these recommendations is given in the next section.

Figure 18. Recommendations for Data Governance Framework for Türkiye

Pillar 1: Policies, Legislation, Regulations

- Recommendation 1.1. Strengthening of a legislative data regime
- Recommendation 1.2. Development of a national data strategy
- Recommendation 1.3. Amending sector-specific regulations and policies
- Recommendation 1.4. Efficient implementation of data protection regulations

Pillar 2: Institutions, Mechanisms, Processes

- Recommendation 2.1. Strengthening leadership in the data-ecosystem
- Recommendation 2.2. Enhancing institutional mechanisms
- Recommendation 2.3. Development of an efficient communication mechanism
- Recommendation 2.4. Setting up a monitoring and evaluation system

Pillar 3: People

- Recommendation 3.1. Implementing capacity development programmes
- Recommendation 3.2. Revising human resources policies
- Recommendation 3.3. Strengthening the data culture
- Recommendation 3.4. Developing data literacy

Pillar 4: Technology anf Infrastructure

- Recommendation 4.1. Use of open-source software and ecosystem solutions
- Recommendation 4.2. Effective implementation of APIs
- Recommendation 4.3. Use of open source data exchange layers
- Recommendation 4.4. Developing cloud infrastructure
- Recommendation 4.5. Further use of analytics and data management tools
- Recommendation 4.6. Further improvement of data standardization
- Recommendation 4.7. Strenghening metadata management and developing data catalogues

Pillar 5: Partnership

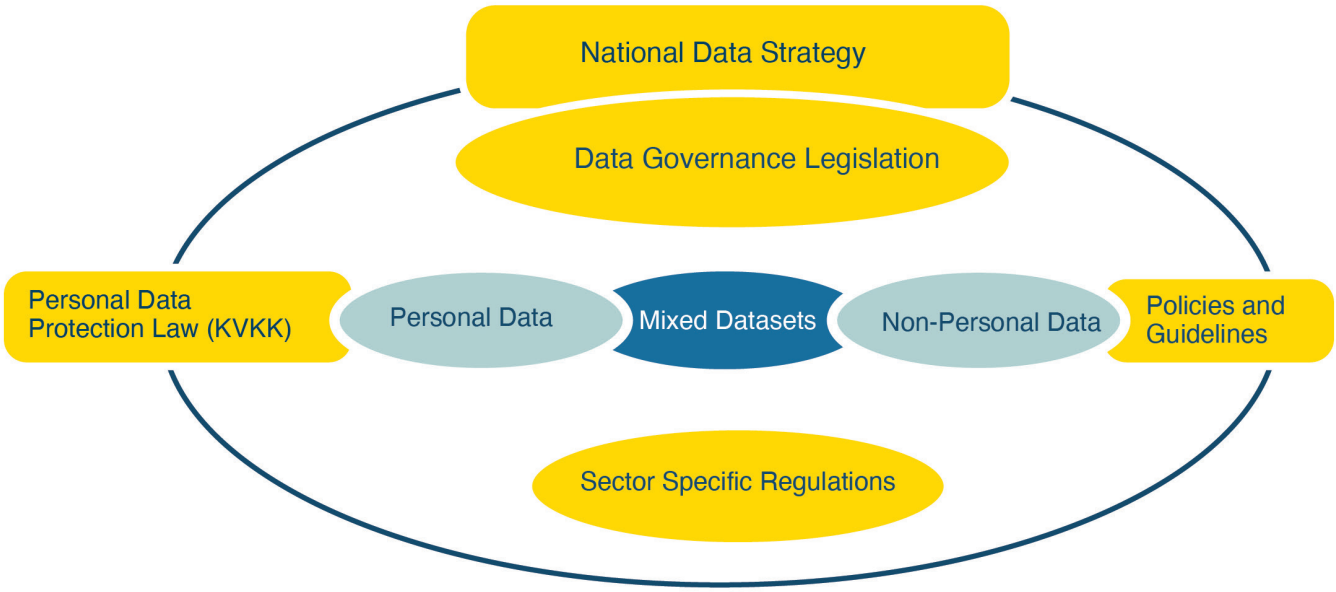
- Recommendation 5.1. Enhancing data sharing arrangements
- Recommendation 5.2. Improving collaboration among the stakeholders
- Recommendation 5.3. Further integration with other data ecosystems

2. Pillars and elements

Pillar 1: Policies, legislation and regulations

To ensure effective data governance and protection of personal information, Türkiye should establish clear data governance policies, legislation and regulations. By implementing these Türkiye can encourage responsible data sharing. These should align with international best practices while considering Türkiye's specific needs. As it is shown in the Figure 19, recommendations under this pillar include the following steps:

Figure 19. Illustration of proposed components for data governance policies and legislation



Recommendations

1.1 Strengthening of a legislative data regime: In line with Türkiye's national priorities and international requirements, it is necessary to strive for alignment with global and regional regulations and establish a path towards the full harmonization of Türkiye's data legislation with them. This process involves a careful evaluation of various legal approaches from other countries, with Türkiye determining its stance by considering international norms and standards. Considering Türkiye's long-term goal of becoming a member of the EU, this must include consideration of pathways to compliance with EU legislation. The principles contained in the EU's Data Governance Act and EU Data Act should be considered alongside goals which have been set by Turkish government strategies and policies.

The legislative changes which this will require also represent an opportunity for Türkiye to establish its own customized data regime that reflects the will of its people and is appropriate to Türkiye's specific context and circumstances, including its current and expected future level and type of technological infrastructure. All stakeholders need assurance that the regulatory framework will be predictable, reliable and equitable at all stages of its development. The following points are specifically recommended:

- **Framework legislation for data governance** should be passed to reconcile discrepancies created by many existing institutions having their own unique regulations. The framework law should also bring in standardized rules for data sharing between organizations and preferably ease processes for sharing data among government organizations.

- **The preparation of a data sharing governance framework**[149] is also recommended. This will set out a collective commitment to proactive, simpler and faster data sharing. In addition, each institution should draft an organisational data sharing policy or plan, setting out how they will implement the framework within their institution.

1.2 Development of a national data strategy and measurable action plans, supported by clear and actionable guidelines and standards. This strategy will ensure appropriate task and responsibility allocation within the data ecosystem and support making data findable and accessible. The national data strategy should be developed with the wide participation of all stakeholders in the data ecosystem.

Practical action plans and projects for public sector institutes: The data strategy needs to be implemented through annual and measurable action plans. These will identify and prioritize data management activities and develop priority use cases for a given year. Institutions can then build on progress from year to year; this will ensure focused, measured progress, and create opportunities to improve and adapt plans. These action plans will also align with ongoing programmes implemented by the central data management office (as proposed under Pillar 2: Institutions, mechanisms and processes, below). The central office can also coordinate these plans to ensure that they complement central policies and the overall strategy and are compliant with statutory requirements. Setting realistic targets that align with the capacities of each institution and taking an integrated approach where institutional projects are mutually supporting will ensure demonstrable steady progress.

1.3 Amending sector-specific regulations and policies: As organizations around the world are embracing cloud technology to drive innovation and improve security, sector specific regulations and policies should likewise welcome it and lay the necessary groundwork for its application, particularly in critical sectors.

Various sectors already have regulations governing data sharing and protection. It is therefore of critical importance that Türkiye revise these regulations to abolish strict data and system localization requirements and so enable increased data sharing:

- Türkiye should ensure that **sector-specific regulations align with broader data governance policies and comply with international standards**. These regulations and policies can include specific guidelines for data protection and security measures relevant to those industries and should seek to close the gap between the law and its practice.
- The **impact of sector-specific legislation** including administrative registers and privately held databases on other sectors or stakeholders **should be assessed through a multi-stakeholder led risk-benefit analysis.** In addition to this comprehensive assessment, government institutions should run a **data sharing risk assessment model**[150] to consider forms of risk to non-personal data that go beyond data sensitivity. For example: the model could consider which organizations the data will be shared with, how it will be shared and what it will be used for. The model should be consistent across government bodies, flexible enough to adapt to changing demands and priorities and should consider and articulate the impact of not sharing data.
- Additionally, the EU Data Governance Act which provides a framework to enhance trust in voluntary data sharing for the benefit of businesses and citizens can act as a guide in strengthening data legislation of Türkiye. It covers various aspects, including data re-use (which enables the re-use of protected data held by public sector bodies), data intermediation

[149] United Kingdom Central Digital and Data Office, Data Sharing Governance Framework (2022), https://www.gov.uk/government/publications/data-sharing-governance-framework/data-sharing-governance-framework
[150] Ibid

services (data intermediaries connect dataproviders with users and cannot monetize data and data altruism (making data available to the Turkish data ecosystem for the benefit of the public).

- B2G (Business to Government) Data Sharing and G2B (Government to Business) Access to Public Sector Data should be also defined. The European Strategy for Data[151] and Data Act[152] of the EU can be used as a source of inspiration when drawing up these definitions.
- It is also recommended to create well-defined protocols and guidelines, and the standards to govern these protocols. These should encompass the terms, rules and procedures required for ensuring the secure exchange of data among ministries and other stakeholders.

1.4 Data protection policies and regulations for the management of personal and non-personal data should be effectively implemented. These policies should consider human rights, particularly children's rights whose personal data requires specific protection. The policies also need to ensure the protection of commercial secrets and have regard for the sector-specific nature of certain types of data. Türkiye could benefit from carefully considering different legal approaches with a view to amending its KVKK in a manner that ensures stricter protection of personal information and takes into account relevant international rules and standards.

Türkiye's stakeholders recognize the importance of the KVKK in establishing a legal foundation for the handling of personal data. However, there is a need to build upon it through guidelines and standards to assist teams in understanding their policy responsibilities and so fully harness the potential of data. Further development of policies and regulations would also help ensure data governance incorporates the requirements of the Data Governance Act, Data Act and other relevant legislation:

[151] European Union, Data Strategy (2020), https://eur-lex.europa.eu/legal-content/EN TXT/?uri=CELEX%3A52020DC0066
[152] European Union, Data Act (2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN

- **A comprehensive legislation assessment is recommended.** This assessment should be made by engaging a broad spectrum of stakeholders including government entities, private sector organizations and civil society. To adopt a comprehensive interdisciplinary approach, a multidisciplinary team should be created with a mix of legal, technological, ethical and policy expertise. The assessment should include the following elements:
  - The formation of a multi-stakeholder committee.
  - Preparation of an inventory of relevant legislation in Türkiye.
  - Further review of relevant legislation and regulations such as the Banking Regulation, Electronic Communications Law, competition laws and all other laws that address improper data access or speak to the principles of protection and privacy.
  - Further review of the Data Governance Act and EU Regulation (EU) 2018/1807 on the free flow of non-personal data in the EU. Place the focus on voluntary data sharing which benefits both businesses and citizens and determining the suitability of such arrangements for Türkiye.
  - In-depth risk assessment in collaboration with various stakeholders, including legal advisors.
- **The tools should be developed** to ensure the secure exchange of data and to empower citizens with the capacity to manage the permissions and consents associated with their data. The concept of data altruism could inform this approach:
  - The EU Data Governance Act[153] references data altruism. Article 16 of this Act defines it as the voluntary sharing of data based on the consent of the data subject (for personal data) or permission of the data holder (for non-personal data). A common European consent form for data altruism streamlines this process which is administered by registered data-altruism organisations. This concept aims to make data available for what the Act considers "objectives of general interest" such as healthcare and scientific research.
- The legal uncertainty resulting from Türkiye's current patchwork of data regulations should be reduced through **non-legislative measures** in order to establish standardised data protection practices. While not limited to these examples, measures could include:
  - Strengthening the national supervisory authority role of KVKK.
  - Publishing additional secondary regulations and guidelines.
  - Further training and awareness raising activities regarding existing regulations and guidelines.
  - Adopting the concepts of data protection by design and by default. This means an assumption data needs to be protected is incorporated into the design and development of products, services and systems from the outset.
  - Devising DPIA tools that help service teams fulfil their obligations. Conducting DPIAs for high-risk data processing activities thereby identifying and mitigating potential privacy risks.
  - Enforcing VERBIS to ensure data controllers are properly managed and comply with data protection regulations.
  - Promoting the principles of ethical and fair use of data.
- While the cross-border flow of personal data from Türkiye is subject to some regulation, practical issues have led to international data sharing faces challenges. As the current system is not working as well as it could there is a need to **update Türkiye's data protection regulations as they relate to cross-border data flows.** The GDPR provides a multi-faceted mechanism allows for much greater flexibility in cross-border data exchange. Türkiye can therefore consider harmonizing its data protection regulations with the GDPR, which would allow the nation to take advantage of this mechanism.

[153] European Union, Data Governance Act (2022), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868

- The KVKK can be revised to this end:
  - Such an **update may include generating a list of countries which can be considered to have sufficient data protection standards to fall within the exceptions offered by article 9 of the KVKK.** It could then define criteria and boundaries for services that can be obtained from international service providers provided those providers are regulated within a state on the secure countries list.
  - Türkiye can **integrate the processing conditions outlined in the GDPR into its KVKK.** This would help data controllers determine the legal basis for cross-border data flows, and give consideration to factors such as the purpose, quality and intensity of the flows.
- An independent institution or agency can **conduct data adequacy assessments** for flows of personal data from Türkiye.
- The **use of alternative data flow mechanisms can be reviewed** to ensure that flows of personal data outside Türkiye are appropriately protected.
- Türkiye can seek positive adequacy decisions from international bodies such as the European Commission. An adequacy decision would acknowledge that Türkiye's data protection laws provide an adequate level of protection for cross-border exchanges. This would enable more fluid exchanges.[154]
- Türkiye can explore the possibility of entering into **mutual recognition agreements** with countries that have strong data protection regimes. These agreements would recognize each other's data protection standards, enabling smoother cross-border data flows.
- Türkiye can introduce **standard contractual clauses** similar to those used in the EU. These clauses would make it straightforward for data exporters and importers to agree to adhere to data protection requirements.
- **A distinction can be made between personal data and non-personal data and** between critical data and non-critical data. **Different regimes can be established for these categories.** This would benefit commerce, enhance data localization, speed up the free flow of non-critical non-personal data across international borders and mitigate the future emergence of additional regulatory hurdles.

Pillar 2: Institutions, mechanisms and processes

Drawing insights from successful data governance practices in other countries is particularly valuable in this area. Challenges around data sharing are amplified by a narrow focus on institutions themselves; a more productive approach is to consider what might be possible if data sources were pooled. In Türkiye there is a particular need to strengthen institutional mechanisms and improve the cataloguing and indexing of data to reduce duplication and improve data quality.

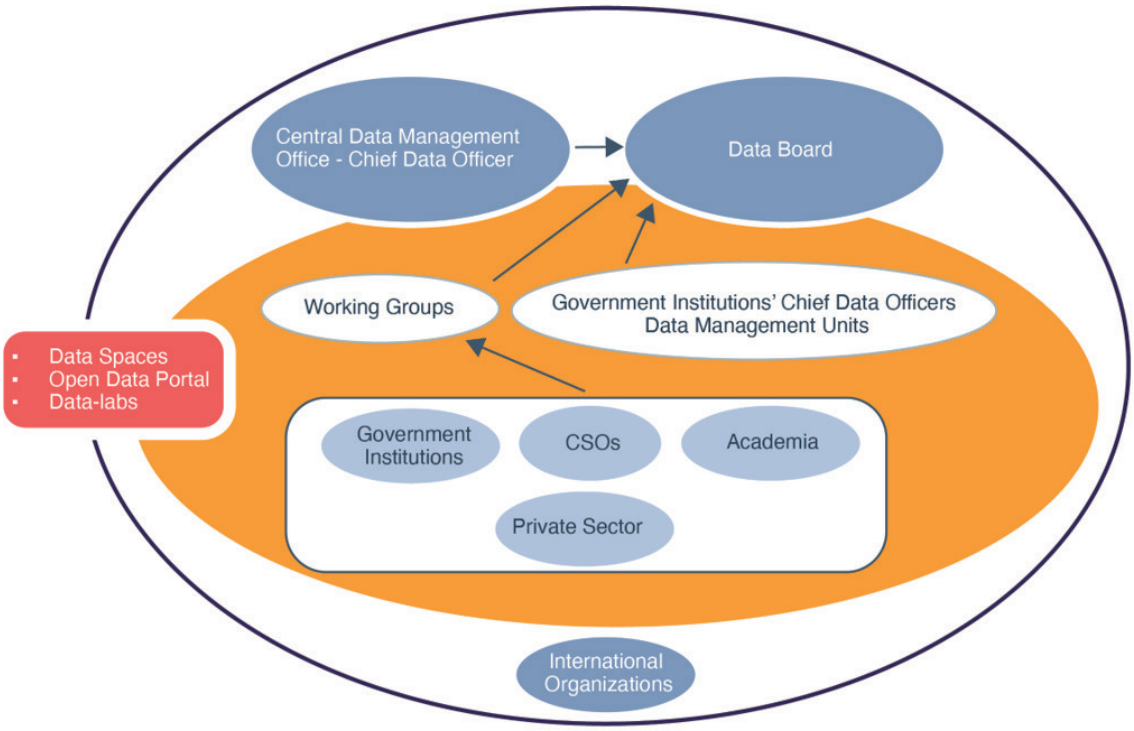
A structure and decision-making process should be established to guide data access, sharing and interoperability. This structure should involve relevant stakeholders and ensure transparency, accountability and compliance with data governance policies. TurkStat's experience in the governance structure of TSS should be drawn upon when creating such mechanisms, suggestions for which are included below.

A successful governance model for the data ecosystem outlines the duties and authorities of the ministries and institutions involved, and incorporates coordination mechanisms for involving the private sector, CSOs, academia and other stakeholders.

Figure 20 shows a proposed structure for this model:

[154] United Kingdom, Department for Digital, Culture, Media & Sport, National Data Strategy (2020), https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy

Figure 20. Proposed institutional and coordination mechanisms for data governance



With respect institutions and processes, UNDP proposes the following components:

Recommendations

2.1 Strengthen leadership in the data-ecosystem: This recommendation incorporates data leadership and stewardship. Roles and responsibilities for data management, including data governance leaders and stewards (individuals who oversee data-related initiatives and ensure adherence to data governance policies), should be assigned. Higher authorities should be specified in legislation and allocated responsibility for the issues of interoperability, use, security and confidentiality.

- **Establish the role of Chief Data Officer:** This can also inspire the establishment of a data board, council or similar body to drive the effective data governance agenda. The commitment of leadership in the national data-ecosystem should be sought, ideally at the highest level of government. A proposed Data Board could be chaired by the Chief Data Officer with a membership encompassing the Chief Data Officers from all relevant ministries and other government institutions and members representing a wide range of views from across industry, academia, the legal sector, representative groups from all sectors of society and technical experts. This board formalizes sustainable governance approaches in the form of a structure through which data management standards and guidelines can be developed and implemented. Such a board will also play an advisory role in ensuring the data strategy remains on track.

2.2 Developing institutional mechanisms at the national level to facilitate data-driven decision-making. These mechanisms involve the establishment of dedicated entities, boards, working groups, frameworks and processes that promote the exchange of data and enhance its utilization in decision-making processes. Various approaches can be taken:

Figure 21. Various approaches towards institutional mechanisms

Top-Down Approach: The leadership of an organization or government sets the vision and mandates the establishment of institutional mechanisms. They define the structure, roles and responsibilities, and allocate resources accordingly. This approach ensures centralized coordination and accountability.

Bottom-Up Approach: Where individuals or working level teams within an organization initiate the establishment of institutional mechanisms. They recognize the need for improved data-driven decision making and work collaboratively to propose structures and processes. This encourages grassroots innovation and allows for flexibility and adaptation to evolving needs.

Hybrid Approach: Combines elements of top-down and bottom-up approaches. The leadership provides the vision and support, while individuals or working level teams contribute their expertise and insights to shape the mechanisms. This approach encourages a sense of ownership and participation from stakeholders at all levels.

Source: UNDP[155]

Türkiye can use a hybrid approach which combines elements of top-down and bottom-up approaches as outlined in Figure 21.

- **Design of a central data management office:** A specific body responsible for overseeing the strategic management of data can be set up. It would be responsible for framing, managing and periodically reviewing and revising data policy. The central data management office shall be responsible for developing rules, standards and guidelines. The co-leadership of the DTO, TurkStat and Personal Data Protection Authority in the data-ecosystem can be incorporated within this new organizational structure.

This central data management office could act as a catalyst by fostering partnerships and by pooling budget and scarce data talent to implement projects. It can act as a governing body by establishing rules for data governance and data quality management as well as defining and sharing data-management best practices and supporting public-sector entities to create their own action plans.

It could oversee the implementation of the data strategy by establishing primary use cases and coordinating capacity development activities towards them. This central data management office can provide insights into the development of data governance policies, standards and platforms.

The responsibilities of this office would include data storage and retention, data quality standards, data security and managing dataset access platforms. The office can own and manage central data architecture, thereby establishing a common data-exchange infrastructure. By establishing standardized components that are useful across a range of use cases government data can be de-siloed and can be made interoperable at scale.

The duties of the central data management office can be outlined as part of the national data strategy. In addition to the core tasks above, this office could take on the following responsibilities:

[155] UNDP, Data to Policy Navigator (2023), https://www.datatopolicy.org/

- Formulate any new data/dataset/metadata rules, standards and guidelines that are required as comprehensively as possible to avoid any duplication. This work should be conducted in consultation with relevant ministries, the private sector and other relevant stakeholders.
- Help government institutions define their data storage and retention framework- particularly on the cloud.
- Finalize standards that cut across sectors.
- Publish and ensure compliance with domain-specific metadata and data quality standards for ministries and government institutions.
- Manage the open data portal and take responsibility for further developing it.
- Coordinate closely with line ministries, and other schematic programmes to standardize data management by building up capacity and capabilities within each ministry.
- Set and publish data anonymization standards and rules to ensure informational privacy is maintained.
- Accelerate the process of sharing non-personal datasets housed with ministries and private companies.
- Management and maintenance of the central data architecture.
- Coordination of prevention work to avoid data breaches.
- Training and sharing best practices across government institutions and stakeholders.
- Provide advice to the ministries and where appropriate represent Türkiye itself in international relations that pertain to data issues.
- Oversee the implementation of the Data Strategy and specific development plans and projects which require central management.
- Participate in the development of legislation, run consultation processes on legislation and advise government institutions, the private sector and the public on interpreting legislation.
- Encourage and foster data and AI-based research.
- Notify stakeholders regarding protocols for the sharing of non-personal datasets while ensuring privacy, security and trust.
- Hold the right to decide whether requesting entities may be allowed access to certain databases and datasets or combinations thereof.
- Clearly define data sharing periods.[156]

[156] India, India National Data Governance Framework Policy (2022), https://www.meity.gov.in/writereaddata/files/National-Data-Governance-Framework-Policy.pdf

- **Redesign of data management units in the ministries and institutions:**
  - Every ministry or government institution could have data management units headed by designated Chief Data Officers who work closely with the central data management office in addition to those in core ministries including the Ministry of Interior and the Ministry of Labor and Social Security. Chief Data Officers should develop their institutions' internal governance structures for the management and use of data. At each institution, the Chief Data Officers can begin the critical steps required to build data strategy road maps proposed under Pillar 1: Policies, legislation and regulations. They can further develop plans for making greater use of data assets, plan capital expenditure on data infrastructure and implement programmes recommended by the central data management office.
  - Data management offices in the ministries should be staffed by a dedicated government data management and analytics unit consisting of staff with data analysis and IT skills. Job descriptions for data analysts, data engineers and data scientists should be prepared for these positions.
  - Municipalities and provinces would also be encouraged to designate or appoint Data Officers.
  - The roles and responsibilities of other officials including data controllers can be further clarified.

- **Establishment of national data council or board:** As suggested above under recommendation 2.1, the National Data Board will be responsible for fostering information-sharing and cross-agency collaboration among the chief data officers of government institutions. Feedback from stakeholders will be used to highlight key topic areas for annual action plans. These plans will build on the progress made by the institutions and the Board to leverage the full value of data, as defined according to the country's values, the board's mission and the public good.

  The Data Board could also do the following:
  - Regularly meet to establish government-wide best practices for the management, use, protection, dissemination and generation of data.
  - Promote and encourage data sharing agreements between institutions which respect their trade secrets and institutional rules.
  - Identify ways in which agencies can improve upon the production of evidence for use in policymaking.
  - Consult with the public and engage with private users of data and other stakeholders on how to improve access to data assets.
  - Identify and evaluate new technology solutions for improving the collection and use of data.

- **Formation of an inter-agency working groups** which adopts multi-stakeholder participation in the data ecosystem. This group should include DTO, TurkStat, the Central Bank of Republic of Türkiye (CBRT), ministries, other government institutions, CSOs, academics, the private sector, the media, policymakers and other stakeholders. Multi-stakeholder working groups on specific themes and subjects bring together individuals with specialized knowledge and expertise to address specific challenges, initiatives or projects or develop strategies, guidelines and protocols. Pre-existing mechanisms enable a more rapid response and greater agility than ad hoc task forces. A list of stakeholders for data governance is given in Table 2:

Table 2. Stakeholders for data governance

Stakeholder group	Stakeholders	Requirements
Government Institutions	Ministries, institutions, municipalities.	▪ Establishing mechanisms in data governance through transparency, engaging civil society, holding all stakeholders accountable for responsible data practices. ▪ Transparency in communicating data laws and policies. ▪ Ensure compliance with data governance policies and legislation.
Civil Society Organizations	NGOs, advocacy groups relevant to the issue.	▪ Representing communities' needs and interests by supporting their participation in data governance. ▪ Advocating for transparency and data privacy.
Academia	Universities, research institutions, think tanks.	▪ Contributing to data governance research and development. ▪ Providing expertise and insights into best practices. ▪ Support education and training programmes on data governance.
Private Sector	Businesses, industry associations, trade groups holding data relevant to the issue.	▪ Engaging in cross-sectoral partnerships and contributing data for social good. ▪ Implementing data protection measures and ensuring data security. ▪ Collaborating with governments and other stakeholders to support responsible data use.
International organizations	UN Agencies, EU, the World Bank, other development partners.	▪ Providing resources and expertise in data governance.[157]

Source: UNDP[158]

Within a task force, members are typically assigned specific roles and responsibilities based on their expertise, experience and the group's objectives. Common responsibilities include a) leading overall direction of the task force (in the case of the chairperson), b) sharing subject matter expertise and data, c) planning initiatives and next steps, d) stakeholder liaison and e) communication and outreach.[159]

[157] Global Partnership for Sustainable Development Data, https://www.data4sdgs.org/taxonomy/term/634 (accessed on 30 August 2023)
[158] UNDP, Data to Policy Navigator (2023), https://www.datatopolicy.org/
[159] UNDP, Data to Policy Navigator (2023), https://www.datatopolicy.org/considerations/develop-institutional-mechnisms-for-continued-use-of-data#governance-of-multistakeholder-groups

International organizations including development partners or other relevant stakeholders can be invited to some meetings as an observer or special guest.

The proposed central data management office can undertake the leadership of these working groups. The co-leadership of the DTO, TurkStat and Personal Data Protection Authority will be essential in managing these working groups. The experience of TurkStat with the working groups of OSP is valuable, Türkiye should benefit from this experience and leverage pre-existing mechanisms when creating inter-agency working groups.

It is good practice to establish the frequency of meetings and other terms of reference at the outset, while keeping in mind that some operational flexibility will be needed. Organization of regular meetings with stakeholders promotes inclusive representation and deeper engagement.

- **Government agencies can be connected through a "Public Data Space" and establishing dedicated units within governmental organizations** can allow those units to act as central hubs for data expertise, research and cooperation. These units can offer advisory services and assist in data-driven initiatives throughout government.
- **Establishment of 'Data-labs' for high-priority use cases:** Strategies take time to achieve results. At the same time, high priority use cases require excellent data management from day one and cannot wait for transformational change to occur. Furthermore, for a strategy to have impact there needs to be trust in the process, which requires positive results, which are difficult to achieve until the strategy has taken effect. For this reason, early success can lead to a virtuous circle whereby stakeholder support for the strategy breeds a successful strategy which breeds further increased trust. Conversely, delayed implementation or early setbacks can set off a vicious cycle whereby stakeholder support is undermined, the strategy becomes harder to implement and further delays lead to further lack of trust. Therefore, in parallel with long term and holistic efforts to modernize the data landscape, governments need to focus on rapid, tangible impact. An effective mechanism for doing this is provided by so-called "data labs"—agile teams with cross-functional expertise that work on ensuring high performance delivery of data for specific high priority use cases. Having developed, tested and finessed solutions to specific issues these solutions can then in many cases be rolled out nationally. Further, this process helps governments identify gaps in their data landscapes such as key but missing datasets or holes in data infrastructure.
- The open data portal can serve as a crucial institutional mechanism to encourage data-driven decision-making and enhance transparency and accountability. Türkiye can efficiently utilize this platform, enabling all stakeholders in the data ecosystem to not only publish and share their data with the public but also with one another. This portal can be managed by the central data management office.

2.3 Developing an efficient communication mechanism or plan across the public sector to promote a shared vision and understanding of the data agenda. This includes supporting institutions in applying data to generate value by establishing communities of practice which allow data professionals to share best practices, address common challenges and develop solutions. This will also increase the amount of research on data undertaken by academics, researchers and policymakers in ministries. The media is also a key partner and can help promote the use of data.

2.4 Setting up a monitoring and evaluation system: There is a need to create mechanisms for monitoring and evaluating the implementation of data governance policies and practices. This may include regular audits, compliance checks, objectively verifiable indicators, a reward system and penalties for non-compliance. This will also ensure continuous improvement and adaptation of the national data governance structure, allowing it to remain flexible with respect to emerging technologies and evolving data governance challenges, ensuring Türkiye keeps pace with global best practices and the changing data landscape.

Additionally, a Data Maturity Assessment[160] for government institutions is recommended to help public sector organisations to measure, improve and maintain the health and strength of their data ecosystems.

Pillar 3: People

People are a crucial pillar of data governance. Guidelines and principles for achieving the ethical treatment of data can be beneficial in helping staff understand their responsibilities. Transparency and accountability in data handling should be improved, including by creating mechanisms for users to manage their data permissions and practical tools for consent giving. Such a change requires improving the following elements which fall under the People component of the data governance framework:

- Understanding and appreciation of data's value in generating public value,
- Making use of data in designing and delivering public services, and
- Using real-time data to meet public needs and improve the capacity of public servants.

By focusing on capacity development and training, and thereby strengthening the data culture and data literacy, Türkiye can build a solid foundation for its data governance framework and foster a data-driven society. Figure 22 illustrates steps to support these objectives:

Figure 22. The people pillar of the recommended data governance framework

Recommendations

3.1 Implementing capacity development programmes: This is essential. These programmes should target government officials, the private sector, academia and CSOs aiming to raise awareness about the importance of data governance and encourage adherence to best practices in Türkiye. Stakeholders can be supported in applying data to generate value by establishing communities of practice, investing in training and resources, defining standards for data sharing and incentivizing data application. Investments in training and capacity development initiatives will enhance data management skills and promote a data-driven culture.

[160] United Kingdom, Data Maturity Assessment for Government (2023), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1143860/Data_Maturity_Assessment_for_Government_-_FINAL_PDF.pdf

Türkiye should also address the specific challenges it faces regarding data governance, particularly in terms of knowledge on personal data, gaps in information on available data and the need for guidelines and reference documents. By investing in capacity development and training, Türkiye can foster a skilled workforce that can leverage data effectively, promote innovation and ensure the responsible use of data. This workforce will then be able to create comprehensive guidance on personal data handling, data availability and the processes for accessing, producing and processing data:

- Guidelines and reference documents: Clear guidelines and reference documents should be developed to provide individuals with information on data access, production and processing. These resources should outline the procedures, standards and regulations related to data governance in Türkiye.
  - Implementation manual: Detailed implementation guidelines including a data sharing toolkit, operational manuals and mechanisms for data anonymization and privacy should be created. In each government institution, technical documents need to be prepared to strengthen institutional memory.
  - The functioning of the National Data Dictionary can be improved. Training should be provided on using this glossary.
  - Project guidelines can be prepared for IT and data projects.

- **Development of data-related skills and competencies** should be increased. Particularly for competencies regarding data standards, data management, data analytics (with a focus on innovative services and products), data security and privacy. This requires addressing the following areas:
  - Data-related skills and competencies: Efforts should be made to develop and enhance these for individuals working with data. This includes providing training on data analysis, data visualization, data modelling and other relevant data-related skills.
  - Data standards: Establishing and promoting data standards is essential for ensuring consistency and interoperability across different datasets. Training programmes should focus on familiarizing individuals with relevant international data standards and encouraging their adoption.
  - Data management: Training initiatives should cover various aspects of data management, including data collection, storage, organization, quality assurance and documentation. This will help individuals understand best practices for managing data effectively.
  - Data analytics: Building capabilities in data analytics is crucial for unlocking insights and deriving value from data. Training programmes should focus on data analysis techniques, statistical methods, machine learning and data-driven decision-making. To reach larger audiences, this process can be conducted in cooperation with relevant ministries and institutions including the Ministry of National Education.
  - Data security and privacy: Individuals need to be trained on data protection measures, encryption techniques, compliance with data privacy regulations and ethical considerations related to data usage.

3.2 Revising human resources (HR) policies: These policies play an important role in fostering and supporting cultures of trust, fairness and inclusion. HR policies provide frameworks within which consistent decisions based on the organizations' core values are made, and promote equity in how people are treated.

Leadership from senior officials and effective governance will be key to establishing a data culture across government, but everyone, regardless of seniority or profession, should see data as a priority in their role – with data supporting each step of policy and delivery, from scoping to ongoing performance tracking, evaluation and lesson learning.

Further measures can be undertaken as follows:

- Prioritise bringing in and building the right skills; consider the competencies of staff across government.
- Recruit leaders with data and digital skills to build a strong cadre of technical, policy, legal and analytical data experts in the centre of government.
- Train a target number of analysts across the public sector in data science by a target year.
- Review data training available to all civil servants and develop proposals to enhance and extend this offering.
- Design a career pathway for data expertise in government, which it could be accommodated within a cyber security vocational school.
- Prepare an action plan for newcomers.
- Allow for and promote hybrid work conditions to attract the workforce with the right skills.
- Agree a shared definition of data expertise across central government and employ qualified data experts in each public institution. Affiliate them with the proposed central data management office.
- Develop a strategy or policy for IT staff recruitment, retention and skill development.
- Establish cross-government communities of practice for data professionals to share good practices, identify common challenges and develop shared solutions.
- Provide all public servants with a grounding in digital government user skills. Ensure that this covers the trustworthy use of data and technology and data-driven government.
- Establish an annual prize acknowledging and rewarding the successful application of data to generate public value and highlighting innovative practices regarding the use of data for anticipation and planning, delivery or evaluation and monitoring.

3.3 Strengthening data culture: This involves creating an environment where data-driven decision-making is encouraged and valued.

Data culture is an open understanding of data as a resource for a knowledge-based society and a means of facilitating participation by the whole of society. This understanding implies an acknowledgement that knowledge is acquired from data, but that this knowledge can also be critically scrutinised.

The general psychological profile of people in the data ecosystem should be considered in this process. One of the main aspects of “change management” is understanding that people’s general attitudes towards reforms determine their success or failure. Successful change management is key for the sustainable and continuous integration of data into the policymaking cycle. Initiating this scale of institutional change requires a comprehensive and strategic approach, as well as sustained commitment and support from leadership and from stakeholders. Strategies around

building data culture, improving data capacities and facilitating collaboration and partnership all contribute towards this institutional change. A few initiatives that will help to foster this change include the following:

- Identify, engage and invest in potential champions. Identify individuals within the organization or government who have a strong interest in data, analytics and evidence-based decision making. Look for those who have a track record of advocating for data-driven approaches or who possess relevant expertise in data analysis, research or policy formulation. Clearly communicate the vision and goals of data-informed policymaking to potential champions. Help them understand how their support and involvement can contribute to achieving these goals. In addition, provide champions with the necessary resources, support and authority to influence change within their organization or government department.
- Creating use cases is an effective strategy to demonstrate the value and potential impact of data-informed decision making and encourage its scaling within an organization or government department. Document the findings, lessons learned and best practices from the use case. Prepare a comprehensive report or case study that highlights the value, impact and scalable potential.
- Advocate for scaling successful approaches across government utilizing documented results and case studies.

Türkiye can also prioritise the following:

- **Support informed handling of data by citizens of all age groups through various formal and informal educational opportunities:** Facilitate participation and awaken interest in developing data-driven business models. Promote the collection of open data by citizens. Encourage active discussion on data use within the framework of citizen-led science projects and train citizens to become experts. Strengthen the population‘s data skills by conducting a comprehensive survey of these skills and, on the basis of the survey’s findings, make excellent learning opportunities available to everyone according to their needs. In order to create and further develop relevant learning opportunities, comprehensive long-term monitoring of the population’s data skills is required. Some key activities to this end are as follows:
  - Establish a national digital education campaign.
  - Promote the development of open standards, infrastructures and governance models for user-centred, self-determined and data protection-compliant data exchanges. Encourage the networking of digital teaching and learning platforms.
  - Record the population‘s level of data skills by establishing continuous and comprehensive long-term data skill monitoring.
- **Improving data skills in education and vocational training**: All school pupils should learn how to collect, process, assess and use data in accordance with relevant legislation and with respect to data privacy and security. Data skills should be anchored in state syllabuses and prepared in an age-appropriate format. The objective should be to ensure that everyone who completes a vocational training programme or a degree course is also taught data skills to a specified minimum standard. To achieve this, the following measures can be considered:
  - Developing data literacy courses and teaching material and making them openly available to teachers and learners in order to teach data skills sustainably.
  - Setting up master and doctoral programmes in the field of data sciences.
- **Demand for and provision of data skills in private sector and industry:** Actions can strengthen the culture of creating and responsibly using trustworthy data in the private sector to create additional value. This includes supporting companies in training their employees in high demand data skills. Other actions include:
  - Increasing awareness of the data economy among companies and enabling them to use data platforms and participate in data-centric industries.
  - Supporting companies with knowledge of the data economy, data analysis and data-

centric business models. Centres can support and advise companies and employees on developing and implementing innovative approaches to independent learning.
    - A project can be designed to train selected company representatives as company-internal mentors. This process can establish employee-based, internal guidance to support further training. It can further be supported by a regional network and will support and draw support from the development of external guidance on training.
    - The creation of a "data toolbox" for data skills in various areas, e. g. for companies and civil organisations. This toolbox would be prepared centrally by appropriate stakeholders within the digital and data-ecosystem and then made freely available.
- **Data skills in civil organisations:** Civil organisations, clubs and associations should be assisted in developing secure and data protection-compliant means of using data more effectively. The central data management office should promote civil organisations that are dedicated to improving the population's data skills and that prepare non-personal data records and make them freely available to the public as common goods. Actions could also encourage expanding the field of citizen-led science, opening up further data sources for stakeholders looking to use data to improve aid delivery or otherwise support common goods and encouraging stakeholders to collect and publish their own open data.
    - Establish a Civic Data Lab to work on creating iterative, collaborative data exchange structures in the non-profit sector and those working for the common good. The Civic Data Lab can assist project sponsors with collecting, preparing and analysing data as well as by providing training in essential skills.
    - Support non-statutory welfare associations in utilising the potential of digitalization and in developing and trailing innovative solutions in social work. In particular, improve digital and data skills as well as raising awareness of data use.

An organizational culture that is supportive of learning is of fundamental importance. This requires an awareness of not only which methods are most effective, but also a robust understanding of the behavioural science of teaching. The wider culture and environment of an organization impacts learning, this culture is shaped by policies regarding permission to learn and the level of support from managers and peers to implement learning.[161]

3.4 Developing Data Literacy: Data literacy is an essential aspect of data governance. It refers to the ability of individuals to understand, analyse and interpret data effectively. Promoting data literacy should be a priority for the data governance framework for Türkiye. This requires providing individuals with the necessary skills and knowledge to work with data, whether they are government officials, private sector stakeholders or the general public.

To improve data literacy, it is important to develop educational programmes and initiatives that focus on data-related skills and competencies. These programmes should cover areas such as data standards, data management, data analytics (including innovative services and products) and data security and privacy. By enhancing data literacy, Türkiye can empower its citizens to make informed decisions, encourage data-driven innovation and ensure responsible data usage.

It is important for Türkiye to have data skills capabilities in the private sector, from basic data literacy to advanced technical skills. Those with both advanced data skills and sector knowledge will be in particular demand throughout Türkiye, meaning that companies will need to have access to viable training options. There is also a need to build on diversity and mobility initiatives in the workplace to ensure that these skills are available to all and at all levels, and to integrate the provision of data skills with the development of business skills.

[161] Germany, Data Strategy of the Federal German Government (2021), https://www.bundesregierung.de/breg-en/service/information-material-issued-by-the-federal-government/data-strategy-of-the-federal-german-government-1950612

In order to sustainably teach skills for data-based empirical work, particularly to students, data literacy courses and teaching materials need to be developed and made openly available to teachers and learners. Vocational courses and public training centres may be used to create them.

Pillar 4: Technology and infrastructure

Technology and infrastructure play a crucial role in enabling effective data management, data sharing and data security. There is a need to develop better connectivity and data sharing capabilities in Türkiye. Initiatives such as comprehensive base registries that provide centralized datasets, an improved data inventory and the creation of data catalogues are important steps to reduce duplication, foster interoperability and enhance data analysis and application.

A standardised model and common technological approach for sharing data should be developed across the data ecosystem. Within administrations, data infrastructure needs to be designed in line with relevant standards.

Appropriate technical mechanisms should be implemented for data access, such as: access control mechanisms, the ability to download data, APIs and data sandboxes. These mechanisms should balance data accessibility with the protection of individuals' and organizations' rights and interests.

Technology and data infrastructure refers to both the overall structure and the specific components of the technological systems used for data governance. In Türkiye, it is important to establish a robust and scalable technology architecture that supports data-related activities. To support effective data governance, Türkiye should invest in technology and tools that enable efficient data management, sharing and analysis. Digital and data maturity levels can be measured, and a roadmap created to facilitate its rise.

The data governance framework for Türkiye requires new or updated foundational technical components within ministries and government institutions, and in some cases within or provided by private sector actors such as financial services providers. These components include data registers, catalogues, APIs, cloud-based solutions and toolsets for data management and data analytics. Self-service applications, and applications for the use of open data and unconventional data sources should be an area of specific focus as this will ensure a comprehensive and holistic approach to data governance.

The following are characteristics that foundational technical components of a country-wide public data and digital infrastructure should have:

- Autonomous: building blocks provide a standalone, reusable service or set of services. They may be composed of many modules or microservices.
- Generic: building blocks are flexible across use cases and sectors.
- Interoperable: building blocks must be able to combine, connect and interact with other building blocks.
- Iterative evolvability: building blocks can be improved even while being in constant use.
- Openness: building blocks should be open, be that by using open-source software, having a public API, conforming to Open API Specifications or adhering to Rest API design principles.

Certain sets of components have been successfully used together to establish a whole-of-government approach and technology architecture in other contexts. These component sets fall within core Digital Public Infrastructure (DPI)[162] categories. Using components from within these categories creates the underlying rails to facilitate interoperability and reusability between systems and use-cases. DPI categories include:

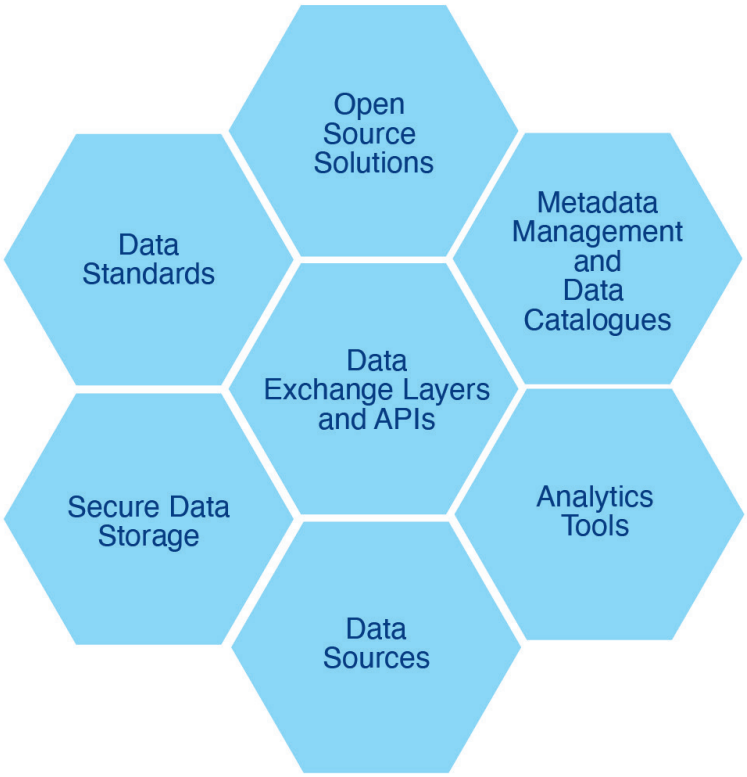
[162] UNDP, Digital Public Infrastructure, https://www.undp.org/digital/digital-public-infrastructure (accessed on 05 July 2023)

- IDs and Registries;
- Electronic Signatures, Public Key Infrastructure, and Trust;
- Data and Credentials, and;
- Discovery & Transactions.

Countries that have been successful in scaling data usage have typically made repeated re-use of these components.[163] For example: ID and registries can be re-used in health, education, financial inclusion, transferring benefits to farmers, object registrations (such as land and carbon) and other areas. This sort of reusability encourages the bringing of data solutions to scale. This same system can also demonstrate interoperability between civil registration and identity, between national ID systems and health ID cards or among social protection registries across various government ministries.

Figure 23 shows the suggested components for Türkiye's data infrastructure:

Figure 23. Proposed data infrastructure components for Türkiye



Recommendations

4.1 Use open-source software and ecosystem solutions which provides unified and secure data exchange between stakeholders in the data ecosystem. Digital Public Goods (DPGs), as defined by the UN Secretary-General, are open-source software, open data, open AI models, open standards and open content. They adhere to privacy and other applicable laws and best practices, do no harm and help attain the SDGs. DPGs are collective digital solutions, freely available for all to modify, add to and deploy. **Well-established, well-supported DPGs and other open-source solutions can be used in Türkiye's data ecosystem.** The "General Directive on the Use of Open-Source Software in the Public Sector" which was recently published (July 2023) aims to promote this approach.

[163] UNDP Accelerating The SDGs Through Digital Public Infrastructure: A Compendium of The Potential of Digital Public Infrastructure (2023), https://www.undp.org/publications/accelerating-sdgs-through-digital-public-infrastructure-compendium-potential-digital-public-infrastructure

4.2 Efficient use of APIs: Implementing APIs enables seamless integration and exchange of data between different systems and platforms. APIs simplify data access and enable efficient and reliable data sharing with external stakeholders, promoting innovation and open data initiatives. Stakeholders are already using the APIs for data sharing; however, Türkiye can focus on the creation of standardised or at least compatible interfaces among its various institutions. In this respect, UNDP recommends **documentation on the specifications of an open API initiative.**[164] Another suggestion is **the creation of technical and data standards for APIs**[165] in addition to broader guidelines for the data ecosystem.

4.3 Use of open-source data exchange layers that allow information to be managed and shared easily but securely among a diverse network of users. Examples include health information exchanges or information management systems, logistics management systems, integrated social registries and integrated financial management systems. For example, Finland, Estonia and Iceland are using X-Road as a open-source data exchange layer solution[166] Similar mechanisms can be established for data sharing among institutions in Türkiye.

4.4 Developing cloud infrastructure: Data needs to be securely stored and communicated to the data provider to instil confidence in data management processes. Türkiye should **develop additional strategies for secure data storage**, including by giving consideration to data backup, disaster recovery and data retention periods. Leveraging cloud-based solutions offers scalability, flexibility, cost-effectiveness, robust security measures, data resilience and accessibility in data storage, processing and management. There is already an **ongoing effort to prepare a cloud strategy** (Public Cloud Computing Strategy[167]) which aims to procure the information technology infrastructure needs of public institutions from commercial cloud service providers to the maximum extent possible. The data storage phase will be more efficient as a result of the **adoption of this strategy and designation of cloud service providers.**

4.5 Further use of analytics and data management tools: Deploying a range of tools for analytics, data management and governance is critical in the whole data ecosystem. These tools include data integration platforms, data quality management systems, **data visualization tools and self-service applications.** Empowering users with diverse toolsets enables efficient data analysis, reporting and decision-making. This requires future readiness, so that emerging technologies such as AI and machine learning, blockchain and the internet of things, etc. can smoothly be deployed to speed up and improve the quality of data collection, processing, verification and analytics.

4.6 Further improvement of data standardization: Implementation of data management practices and standards is needed to ensure data quality, consistency and integrity. Adopting and promoting the use of common data standards across the data ecosystem is important. **Standardized data formats, schemas and classifications facilitate data integration, exchange and analysis**. Aligning with international data standards can enhance compatibility and interoperability with global datasets.

The following points need to be considered with respect to data standardization in Türkiye:

- Unique ID definition: Having a unique ID number for each data unit or variable helps ensure the accuracy and integrity of data. it facilitates the accurate linking and analysis of data across different datasets.

[164] Germany, Data Strategy of the Federal German Government (2021), https://www.bundesregierung.de/breg-en/service/information-material-issued-by-the-federal-government/data-strategy-of-the-federal-german-government-1950612

[165] United Kingdom, Guidance, API technical and data standards, https://www.gov.uk/guidance/gds-api-technical-and-data-standards (accessed on 01 July 2023)

[166] Giulia Guadagnoli, A conversation with Petteri Kivimäki on X-Road, Open Source Observatory (2021), https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/open-source-international-cooperation

[167] Türkiye, Digital Transformation Office of the Presidency of the Republic of Türkiye, Public Cloud Computing Strategy, https://cbddo.gov.tr/en/public-cloud-computing-strategy/ (accessed on 09 September 2023)

- Unit of measurement and definitions: Clearly defining units of measurement and their definitions is crucial for accurate data representation and analysis. Consistent unit definitions across datasets enable meaningful comparisons and reliable data interpretation. Not only the unit of measurement but also the consistency of populations, geographical scope and timeframes need to be considered as part of standardization.
- Concepts and variable definitions: Clearly defining variables and their representations (classifications, code lists and formats) within the data architecture helps ensure consistency and accurate data representation. Standardizing variable definitions can facilitate data integration and analysis across different datasets.
- Addressing data inconsistencies: Handling data inconsistencies is essential for maintaining data quality. This involves identifying and resolving discrepancies or anomalies in data values, formats or structures. Implementing data validation and verification mechanisms can help identify and rectify data inconsistencies.
- Updating data in administrative registers: Establishing processes and systems for regular data updates and synchronization with administrative registers enhances data reliability and relevance. The following issues are critical for administrative registers in Türkiye:
  - Key variables should be accurate and complete so data can be matched with respect to unit base. Common unit definition information and identity keys (identity number, tax register number, address nr. etc.) should be used by all stakeholders.
  - If is appropriate in administrative registers, common variables (e.g., age, gender, job) can be determined and defined, and code lists for these variables can be specified. Thus, each administration register owner can keep their data according to the same standards and share their data with ease (provided data privacy principles are followed).
  - The data standards related to administrative registers in government institutions can be planned by a higher authority (such as the proposed central data management office) on a national basis.
  - Access authorization should be given to agreed users on the basis of agreed factors to ensure data sharing among government institutions.
- Pre-existing standards and ongoing projects (e.g. Public Data Space project, National Data Glossary) can be used and extended to all stakeholders in the data ecosystem.

4.7 Strengthening metadata management and developing data catalogues: Establishing **a comprehensive metadata system** is crucial for documenting and managing data-related information. Metadata should capture details about data sources, data lineage, data quality and other relevant attributes in line with the fundamental privacy principles (e.g. data minimization, storage limitation, integrity and confidentiality). Implementing strong metadata practices can improve data discoverability, understandability and usability.

One of the tools for good metadata management is the data catalogue. Developing data catalogues provides comprehensive information about available datasets, their characteristics and access mechanisms. These catalogues act as central repositories of metadata and facilitate data discovery and sharing.

Metadata management can be strengthened by the following recommendations:

- DTO, TurkStat, the Ministry of Environment, Urbanization and Climate Change and the Ministry of Health can provide **guidance on a metadata management model for the data ecosystem** considering their work on the data dictionary and metadata management.
- TurkStat has an ongoing effort to establish a National Registry System to support inter-institutional interoperability. As part of these efforts, a national standard (TS 13889) covering information technology, national registry systems and national registry requirements has been prepared in partnership with the Turkish Standards Institute. The objective of this effort is to enhance data and metadata collection in crucial areas for the country, ensuring their systematic, secure and up-to-date presentation while fostering better data collaboration

between private and public entities. This **standard should be efficiently implemented by relevant institutions to establish a common understanding.**

- **Training and certification organizations can be established to expand metadata preparation and data exchange** to institutions and businesses.
- Opportunities for enhancing the cataloguing and indexing of data can be created. Data quality can be improved **by supporting organizations in preparing data catalogues.** This includes by developing guidelines for, and improving the quality of, Open Government Data in Türkiye. **The Data Catalogue Application Profile (DCAT-AP) already provides a universal standard** for metadata.[168]
- **AI, machine learning and semantic inference** can be utilized to automate processes for collecting metadata in data catalogues.

Pillar 5: Partnerships

Partnerships are an essential part of the data governance framework for Türkiye as they facilitate data sharing, collaboration and the effective utilization of data.

The e-Government Gateway in Türkiye serves as an effective platform for data exchange. However, there is a need to overcome challenges related to data security concerns and the perception that it is safer to keep data within organizations. Public servants should be given the necessary training to judge appropriate situations for data sharing and collaboration. Enhancing partnerships and encouraging greater sharing of data can help unlock the full value of data, including for the public sector.

UNDP recommends:

- Building trust, transparency and ethical use of data through partnerships and communication efforts.
- Strengthening public trust in the government's handling of data.
- Ethical use and management of data beyond personal data protection.
- Transparency and accountability through tools like VERBIS.
- Equipping the public with tools for managing data permissions and consent.
- Balancing digital security, privacy and public service reliability.
- Training public servants to navigate data tensions and generate public value.
- Balancing partnership structures by including both local and international stakeholders.

[168] European Commission, DCAT Application Profile for data portals in Europe, https://ec.europa.eu/isa2/solutions/dcat-application-profile-data-portals-europe_en/ (accessed on 09 September 2023)

- Data altruism can play crucial role in Türkiye's data governance framework. Encouraging individuals and organizations to participate in data altruism can lead to the collection of valuable datasets for research, policy development and public benefit. By fostering a culture of data altruism, Türkiye can leverage collective data resources to address societal challenges and drive data-driven innovations, all while ensuring data privacy and ethical data use.
- Data intermediaries can play a significant role in facilitating data sharing and collaboration within the data governance framework.

Different data sharing partnerships have individual data-sharing agreements. By joining existing data partnerships together, data collaboratives and data commons can be created.

By establishing data sharing arrangements, fostering collaboration with the private sector and academia, integrating with other data ecosystems, improving national data governance mechanisms and aligning with international standards, Türkiye can build strong partnerships that promote data-driven innovation, problem-solving, and cooperation at the national and international levels.

Figure 24 illustrates the key aspects for such partnerships:

Figure 24. Partnerships pillar of the recommended data governance framework

The following sections highlight key aspects of the recommended framework.

Recommendations

5.1 Enhancing data sharing arrangements: Establishing a data sharing agreement is a key foundation in formalizing a data partnership, which can encompass Public-Private Partnerships (PPPs).

There are different kinds of data sharing partnerships including: **data-sharing agreements** between two parties to share specific data with direct agreement, **data collaboratives** which are often used when private sector data is combined to help inform public sector decisions and **data commons** which is a shared pool of data resources accessible to a defined community of users which provides an environment for collaborative data analysis, experimentation and innovation.

Data sharing arrangements should make provision for:

- Developing a shared data infrastructure that enables secure and controlled access to data across organizations. This infrastructure should incorporate mechanisms for data sharing, access controls, data anonymization and data governance to ensure privacy, security and compliance.

- Creating data collaboration platforms that allow different organizations, both public and private, to collaborate and share data in a controlled environment. These platforms can provide tools for data integration, analysis and visualization, fostering collaboration and knowledge exchange for problem-solving and decision-making.

5.2 Improving collaboration and cooperation among the stakeholders: Government entities can partner with non-governmental organizations, academia or private entities to access data. In fact, most governments have mechanisms for systematic engagement, especially with non-profit organizations.

Collaboration with the private sector and academia is crucial to accelerate analysis, problem-solving and innovation. Türkiye should actively engage these sectors in the data governance framework by establishing:

- Data research partnerships: Establishing research partnerships with academic institutions and private sector organizations to conduct joint data analysis, research and the development of data-driven solutions. This collaboration can bring together domain expertise, diverse perspectives and advanced analytical capabilities for tackling complex challenges.
- Data innovation hubs: Creating innovation hubs or centres that bring together the public sector, private sector and academia to foster collaboration, experimentation and co-creation of data-driven solutions. These hubs can serve as platforms for knowledge sharing, capacity building and fostering a culture of innovation.
- Public-private-academia coordination: As indicated under Pillar 3: People, Türkiye can promote collaboration between the public and private sectors. Establishing partnerships and engaging corporate experts, industry leaders and academics can help bridge the gap between levels of data expertise available in different sectors and drive effective integration and usability of open data. Coordination and collaboration can be facilitated through regular forums, consultations and joint initiatives. This ensures that data governance efforts are inclusive, benefit from diverse expertise and align with the needs of various stakeholders. Public organizations can create roles related to communication, technological innovation and digital transformations (including the adoption of AI, the use of big data analytics and the transition to cloud computing) and appoint members of the private sector or academia to them. This outsourcing can bring advantages, including flexibility.
- Interagency data governance committees: As indicated under Pillar 2: Institutions, mechanisms and processes, creating interagency committees or working groups brings together representatives to harmonize data governance practices, exchange knowledge and resolve data-related challenges collectively. Data practice community groups[169] can be also considered to ensure partnership and collaboration within the data ecosystem.
- Non-public stakeholder engagement: Türkiye could actively involve non-public stakeholders, such as civil society organizations, community groups and industry representatives in the data governance process. Encouraging their participation, feedback and contributions helps address societal concerns, ensures transparency and enhances the relevance and effectiveness of data governance initiatives.

[169] New Zealand, Data practice communities (2023), https://www.data.govt.nz/toolkit/communities-and-groups/

5.3 Further integration with the international community and other data ecosystems: To facilitate cross-border data flows and ensure compatibility with global data governance norms, Türkiye should align its data governance framework with other international standards and frameworks. Activities to this end include:

- Further alignment with international standards: This promotes data protection, privacy rights and interoperability. This can help facilitate cross-border data flows and ensure compatibility with global data governance norms.
- International collaboration: By enhancing international cooperation and partnerships to exchange best practices, share knowledge, collaborate on global data governance challenges, participate in international forums and initiatives and taking up roles on standards bodies, Türkiye can contribute to the development of global data governance norms while benefitting from shared experiences and expertise. Türkiye should prioritize further integration with other data ecosystems by actively seeking partnerships and collaboration with external data sources such as international organizations, research institutions and industry associations. Accessing diverse datasets and integrating them into domestic data can enhance data quality, breadth and depth of insights and facilitate evidence-based policymaking.

Annexes

Annex 1. List of documents reviewed and references

Association of Southeast Asian Nations (ASEAN), Framework on Digital Data Governance (2021), https://asean.org/wp-content/uploads/2021/08/ASEAN-Data-Management-Framework.pdf

Carnegie Endowment for International Peace, Data Governance, Asian Alternatives (2022), https://carnegieendowment.org/files/Data_Governance_v1.pdf

Cyber Risk GmbH, The European Data Act (2023), https://www.eu-data-act.com/

European Commission, DCAT Application Profile for data portals in Europe, https://ec.europa.eu/isa2/solutions/dcat-application-profile-data-portals-europe_en/ (accessed on 09 September 2023)

European Commission, Digital Public Administration factsheet 2022 Türkiye (2022), https://joinup.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2022_T%C3%BCrkiye_vFinal_0.pdf

European Union, Data Governance Act (2022), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868

European Union, Data Strategy (2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066

European Union, General Data Protection Regulation (2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

European Union, General Data Protection Regulation (2016), https://gdpr.eu/tag/gdpr/

European Union, Regulation (EU) 2018/1807 of The European Parliament and of The Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (2018), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807

F. P. Pittman, A. Hafiz, A. Hamm, White & Case LLP, ICLG.com, Data Protection Laws and Regulations USA 2023, https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa (accessed on 12 July 2023)

Gaia-X, https://gaia-x.eu/ (accessed on 30 August 2023)

Germany, Cloud Compliance Center (2023), https://resourcehub.bakermckenzie.com/en/resources/cloud-compliance-center/emea/germany

Germany, Data Strategy of the Federal German Government (2021), https://www.bundesregierung.de/breg-en/service/information-material-issued-by-the-federal-government/data-strategy-of-the-federal-german-government-1950612

Germany, Federal Government, Artificial Intelligence Strategy of the German Federal Government (2020), https://www.ki-strategie-deutschland.de/files/downloads/Fortschreibung_KI-Strategie_engl.pdf

Germany, Federal Ministry of Justice, Federal Data Protection Act (2017), https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html

Germany, Federal Ministry of the Interior, Building, and Community, National data protection law (2023), https://www.bmi.bund.de/EN/topics/it-internet-policy/data-protection/data-protection-node.html

Giulia Guadagnoli, A conversation with Petteri Kivimäki on X-Road, Open Source Observatory (2021), https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/open-source-international-cooperation

Global Partnership for Sustainable Development Data, https://www.data4sdgs.org/taxonomy/term/634 (accessed on 30 August 2023)

India, India National Data Governance Framework Policy (2022), https://www.meity.gov.in/writereaddata/files/National-Data-Governance-Framework-Policy.pdf

International Data Spaces Reference Architecture Model, https://internationaldataspaces.org/publications/ids-ram/ (accessed on 30 August 2023)

McKinsey, Government data management for the digital age (2021), https://www.mckinsey.com/industries/public-sector/our-insights/government-data-management-for-the-digital-age

National Information Society Agency (Jong-Sung Hwang, Ph.D), Korea's Data Ecosystem (2022), https://www.worldbank.org/content/dam/infographics/780xany/2022/apr/Presentations/Korea-s-Data-Ecosystem-20220428.pdf

New Zealand, Data Ethics (2023), https://data.govt.nz/toolkit/data-ethics/

New Zealand, Data practice communities (2023), https://www.data.govt.nz/toolkit/communities-and-groups/

New Zealand, Department of Internal Affairs of the New Zealand, Data and Information Governance (2017), https://www.digital.govt.nz/assets/Standards-guidance/Technology-and-architecture/Architecture-Resources/Data-and-information-goverance-and-maturity/Data-and-Information-Governance-v2.2.pdf

New Zealand, Department of Internal Affairs, Data and Information Governance Toolkit Guidelines (2015), https://www.digital.govt.nz/assets/Standards-guidance/Technology-and-architecture/Architecture-Resources/Data-and-information-goverance-and-maturity/Data-and-Information-Governance-Toolkit-Guidelines.pdf

New Zealand, Government analytics network (2023), https://www.data.govt.nz/toolkit/communities-and-groups/government-analytics-network/

New Zealand, Government Chief Data Steward (2023), https://data.govt.nz/leadership/gcds/

New Zealand, Government Data Strategy and Roadmap (2021), https://www.data.govt.nz/assets/Uploads/4e-government-data-strategy-and-roadmap.pdf

New Zealand, Government Enterprise Architecture (2021), https://www.digital.govt.nz/assets/Standards-guidance/Technology-and-architecture/Architecture-Resources/Data-and-information-goverance-and-maturity/Data-and-Information-Governance-Toolkit-Guidelines.pdf

New Zealand, Privacy Act (2020), https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html?search=ts_act%40bill%40regulation%40deemedreg_privacy_resel_25_a&p=1#LMS23417

New Zealand, Statistics New Zealand (Kevin J. Sweeney), Re-Imagining Data Governance (2018), https://www.data.govt.nz/assets/Uploads/Re-Imagining-Data-Governance_OA.pdf

Organization for Economic Cooperation and Development (OECD), Data governance in the public sector (2019), https://www.oecd-ilibrary.org/sites/9cada708-en/index.html?itemId=/content/component/9cada708-en

OECD, Digital Government Review (2023), https://www.oecd.org/gov/digital-government-review-Türkiye-assessment-and-recommendations.pdf

OECD, Digital Government Review of Argentina (2019), https://www.oecd-ilibrary.org/governance/digital-government-review-of-argentina_354732cc-en

OECD, The Path to Becoming a Data-Driven Public Sector (2019), https://www.oecd-ilibrary.org/sites/9cada708-en/index.html?itemId=/content/component/9cada708-en#endnotea2z34

Petteri Kivimäki (2019), Article: X-Road – a Secure Open Source Data Exchange Layer, https://www.apiscene.io/lifecycle/article-x-road-a-secure-open-source-data-exchange-layer/

Singapore, Government Developer Portal, Data.gov.sg — The One-Stop Open Data Portal for Publicly Available Singapore Government Datasets, https://www.developer.tech.gov.sg/products/categories/data-and-apis/data-gov-sg/overview.html (accessed on 05 July 2023)

Singapore, Infocomm Media Development Authority, Public-Private Data Collaboration Case Study (2019), https://www.imda.gov.sg/-/media/imda/files/programme/data-collaborative-programme/datathon-case-study.pdf

Singapore, Infocomm Media Development Authority, Trusted Data Sharing Framework (2019), https://www.imda.gov.sg/how-we-can-help/data-innovation/trusted-data-sharing-framework

Singapore, Personal Data Protection Act (2012), https://sso.agc.gov.sg/Act/PDPA2012

Singapore, Personal Data Protection Commission, Data Protection Trustmark, https://www.pdpc.gov.sg/overview-of-pdpa/data-protection/business-owner/data-protection-trustmark (accessed on 05 July 2023)

Singapore, Personal Data Protection Commission, Advisory Committee, https://www.pdpc.gov.sg/Who-We-Are (accessed on 05 July 2023)

Singapore, Singapore's national open data collection, https://beta.data.gov.sg/ (accessed on 05 July 2023)

Singapore, Singpass, https://www.singpass.gov.sg/main/ (accessed on 05 July 2023)

Switzerland, Swiss Federal Statistical Office, National Data Management NaDB (2020), https://unece.org/fileadmin/DAM/stats/documents/ece/ces/2020/S8_Switzerland.pdf

Switzerland, Federal Council, New Federal Act on Data Protection, https://www.kmu.admin.ch/kmu/en/home/facts-and-trends/digitization/data-protection/new-federal-act-on-data-protection-nfadp.html (accessed on 07 July 2023)

Switzerland, Federal Data Protection and Information Commissioner, https://www.edoeb.admin.ch/edoeb/en/home.html (accessed on 07 July 2023)

Switzerland, Swiss Federal Statistical Office, Strategy for open government data in Switzerland 2019 – 2023 (2021), https://www.bfs.admin.ch/bfs/en/home/services/ogd/documentation.assetdetail.16164831.html

The World Bank, National Digital Identity and Government Data Sharing in Singapore (2022), https://www.developer.tech.gov.sg/assets/files/GovTech%20World%20Bank%20NDI%20APEX%20report.pdf

The World Bank, World Development Report 2021: Data for Better Lives (2021), https://www.worldbank.org/en/publication/wdr2021

Türkiye, Digital Transformation Office of the Presidency of the Republic of Türkiye, Information and Communication Security Guide, https://cbddo.gov.tr/en/icsguide/ (accessed on 21 June 2023)

Türkiye, Digital Transformation Office of the Presidency of the Republic of Türkiye, National Artificial Intelligence Strategy 2021-2025, https://cbddo.gov.tr/SharedFolderServer/Genel/File/TRNationalAIStrategy2021-2025.pdf (accessed on 21 June 2023)

Türkiye, Digital Transformation Office of the Presidency of the Republic of Türkiye, National Data Dictionary Project, https://cbddo.gov.tr/en/projects/nationaldatadictionary/ (accessed on 21 June 2023)

Türkiye, Digital Transformation Office of the Presidency of the Republic of Türkiye, Open Data Project, https://cbddo.gov.tr/en/opendata/about-the-project/ (accessed on 21 June 2023)

Türkiye, Digital Transformation Office of the Presidency of the Republic of Türkiye, Public Cloud Computing Strategy, https://cbddo.gov.tr/en/public-cloud-computing-strategy/ (accessed on 09 September 2023)

Türkiye, Digital Transformation Office of the Presidency of the Republic of Türkiye, Public Net Project, https://cbddo.gov.tr/en/projects/kamu-net/ (accessed on 23 June 2023)

Türkiye, Geographic Information Systems Law (2020), https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=7221&MevzuatTur=1&MevzuatTertip=5

Türkiye, Law on Right to Information (2003), https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=4982&MevzuatTur=1&MevzuatTertip=5

Türkiye, Ministry of Environment, Urbanization and Climate Change, General Directorate of

Geographic Information Systems https://cbs.csb.gov.tr/en (accessed on 12 July 2023)

Türkiye, Ministry of Environment, Urbanization and Climate Change, General Directorate of Geographic Information Systems, Mevzuat (Legislation) (2021), https://webdosya.csb.gov.tr/db/cbs/icerikler/mevzuat-kitabi-dijial-web-020721-rv-20210702093531.pdf

Türkiye, Ministry of Health, Ulusal Sağlık Veri Sözlüğü (National Health Data Dictionary), https://dijitalhastane.saglik.gov.tr/TR,4887/usvs-ulusal-saglik-veri-sozlugu.html (accessed on 29 October 2023)

Türkiye, Ministry of Transport and Infrastructure, National Cyber Security Strategy 2020-2023 (2020), https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2020-2023.pdf

Türkiye, Ministry of Treasury and Finance, Bütünleşik Kamu Mali Yönetim Bilişim Sistemi (Integrated Public Financial Management Information System), https://muhasebat.hmb.gov.tr/bkmybs-projesinin-amaci (accessed on 29 October 2023)

Türkiye, Personal Data Protection Authority, Data Controllers' Registry Information System, https://www.kvkk.gov.tr/Icerik/6650/VERBIS (accessed on 30 June 2023)

Türkiye, Personal Data Protection Law (2016), https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law

Türkiye, the Presidency of Strategy and Budget, 2022 Annual Presidential Program (2021), https://www.sbb.gov.tr/wp-content/uploads/2021/10/2022-Yili-Cumhurbaskanligi-Yillik-Programi-26102021.pdf

Türkiye, the Presidency of Strategy and Budget, 2024 Annual Presidential Program (2023), https://www.sbb.gov.tr/wp-content/uploads/2023/10/2024-Yili-Cumhurbaskanligi-Yillik-Programi.pdf

Türkiye, the Presidency of Strategy and Budget, Medium Term Program (2024-2026) (2023), https://www.sbb.gov.tr/wp-content/uploads/2023/09/Medium-Term-Program-2024-2026.pdf

Türkiye, the Presidency of Strategy and Budget, The Eleventh Development Plan (2019-2023) (2019), https://www.sbb.gov.tr/wp-content/uploads/2022/07/Eleventh_Development_Plan_2019-2023.pdf

Türkiye, the Presidency of Strategy and Budget, The Twelfth Development Plan (2024-2028) (2023) https://www.sbb.gov.tr/wp-content/uploads/2023/11/On-Ikinci-Kalkinma-Plani_2024-2028_17112023.pdf

Türkiye, Turkish Academic Network and Information Center, https://ulakbim.tubitak.gov.tr/en (accessed on 13 October 2023)

Türkiye, Turkish Statistical Institute, Classification Server (2020), https://biruni.tuik.gov.tr/DIESS/ChangeLocaleAction.do?dil=en

Türkiye, Turkish Statistical Institute, Electronic Data Research Center (EVAM), https://evam.tuik.gov.tr/ (accessed on 30 August 2023)

Türkiye, Turkish Statistical Law (2005), https://www.tuik.gov.tr/Kurumsal/Turkiye_Istatistik_Kanunu

Türkiye, Turksat, Turkish e-Government Gateway, https://www.turksat.com.tr/sites/default/files/2020-07/turkish-e-government-catalog-en.pdf (accessed on 30 August 2023)

UN DESA, Adopting National Data Governance Framework for Sustainable Development (2022), https://publicadministration.un.org/Portals/1/Adopting%20National%20Data%20Governance%20Framework%20-%20W%20Kwok%20July%202022%20FINAL.pdf

UN Human Rights Office of the High Commissioner (OHCHR), Human Rights-Based Approach to Data (HRBAD) (2018), https://www.ohchr.org/sites/default/files/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf

UNDP, Accelerating the SDGs Through Digital Public Infrastructure: A Compendium of The Potential of Digital Public Infrastructure (2023), https://www.undp.org/publications/accelerating-sdgs-through-digital-public-infrastructure-compendium-potential-digital-public-infrastructure

UNDP, Data Futures Exchange, 8 Data Principles for UNDP, https://data.undp.org/who-we-are#principles (accessed on 19 May 2023)

UNDP, Data to Policy Navigator (2023), https://www.datatopolicy.org/

UNDP, Data to Policy Navigator (2023), https://www.datatopolicy.org/considerations/develop-institutional-mechnisms-for-continued-use-of-data#governance-of-multistakeholder-groups

UNDP, Digital Public Infrastructure, https://www.undp.org/digital/digital-public-infrastructure (accessed on 05 July 2023)

UNDP, UNDP Data Strategy (2022-2025) (2022)

UNESCAP, Open Government Data Policies and Practices in the Republic of Korea (2020), https://www.unapcict.org/sites/default/files/2020-07/Open%20data%20policies%20and%20practices%20in%20the%20ROK_FINAL.pdf

United Kingdom, API design guidance, https://www.gov.uk/government/collections/api-design-guidance (accessed on 01 July 2023)

United Kingdom, Central Digital and Data Office, Data Sharing Governance Framework (2022), https://www.gov.uk/government/publications/data-sharing-governance-framework/data-sharing-governance-framework

United Kingdom, Centre for Data Ethics and Innovation, https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation (accessed on 27 June 2023)

United Kingdom, Data Maturity Assessment for Government (2023), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1143860/Data_Maturity_Assessment_for_Government_-_FINAL_PDF.pdf

United Kingdom, Data Standards Authority, https://www.gov.uk/government/groups/data-standards-authority (accessed on 27 June 2023)

United Kingdom, Department for Digital, Culture, Media & Sport (2020), National Data Strategy, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy

United Kingdom, Digital Economy Act (2017), https://www.legislation.gov.uk/ukpga/2017/30/contents/enacted

United Kingdom, Find open data, https://www.data.gov.uk/ (accessed on 21 June 2023)

United Kingdom, Government Digital Service Blog, 'Government as a data model': what I learned in Estonia (2013), https://gds.blog.gov.uk/2013/10/31/government-as-a-data-model-what-i-learned-in-estonia/

United Kingdom, Guidance, API technical and data standards, https://www.gov.uk/guidance/gds-api-technical-and-data-standards (accessed on 01 July 2023)

United Kingdom, Guidance, Make better use of data, https://www.gov.uk/guidance/make-better-use-of-data (accessed on 29 June 2023)

United Kingdom, Guidance, Make things secure, https://www.gov.uk/guidance/make-things-secure (accessed on 29 June 2023)

United Kingdom, Guidance, Make use of open standards, https://www.gov.uk/guidance/make-use-of-open-standards (accessed on 29 June 2023)

United Kingdom, Guidance, Manage your data for access and reuse, https://www.gov.uk/guidance/manage-your-data-for-access-and-reuse (accessed on 30 June 2023)

United Kingdom, Information Commissioner's Office, ICO25 strategic plan, https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/ico25-plan/ (accessed on 21 June 2023)

United Kingdom, Metadata standards for sharing and publishing data, https://www.gov.uk/government/collections/metadata-standards-for-sharing-and-publishing-data (accessed on 30 August 2023)

United Kingdom, NHS England, https://www.england.nhs.uk/ig/about/ (accessed on 27 June 2023)

United Kingdom, Service manual, https://www.gov.uk/service-manual/service-standard (accessed on 27 June 2023)

United Kingdom, UK public sector APIs, https://www.api.gov.uk/#uk-government-apis (accessed on 01 July 2023)

United Kingdom. The Technology Code of Practice, https://www.gov.uk/guidance/the-technology-code-of-practice (accessed on 29 June 2023)

United States of America, The US Government Federal Data Strategy (2020), https://strategy.data.gov/assets/docs/2020-federal-data-strategy-framework.pdf

United States of America, National Institute of Standards and Technology (2023), https://csrc.nist.gov/pubs/sp/800/188/final

Annex 2. List of stakeholders interviewed

(in alphabetical order)

1. Ankara University - Faculty of Economics
2. Association of Electricity Producers
3. Banking Regulation and Supervision Agency
4. Central Bank of the Republic of Türkiye
5. Digital Transformation Office of the Presidency of the Republic of Türkiye
6. DT Cloud
7. Energy Market Regulatory Authority
8. Equinix Türkiye
9. Eskisehir Osmangazi University
10. Gama Energy
11. Hacettepe University, Institute of Population Studies
12. Information and Communication Technologies Authority
13. International Investors Association
14. Istanbul Technical University
15. Istanbul Technopark Management
16. Konya Metropolitan Municipality
17. Ministry of Agriculture and Forestry
18. Ministry of Culture and Tourism
19. Ministry of Energy and Natural Resources
20. Ministry of Environment, Urbanization and Climate Change (Directorate General of Geographic Information Systems, Directorate General for Local Authorities)
21. Ministry of Family and Social Services
22. Ministry of Health
23. Ministry of Industry and Technology
24. Ministry of Interior and Directorate General of Migration Management, General Directorate of Population and Citizenship Affairs)
25. Ministry of Justice
26. Ministry of Labor and Social Security
27. Ministry of National Education
28. Ministry of Trade
29. Ministry of Transport and Infrastructure
30. Ministry of Treasury and Finance
31. Ministry of Youth and Sports
32. Personal Data Protection Authority
33. Presidency of Strategy and Budget
34. Scientific and Technological Research Council of Türkiye
35. Social Security Institution
36. Turkish Industry and Business Association
37. Turkish Statistical Institute
38. Union of Chambers and Commodity Exchanges of Türkiye
39. Union of Turkish Municipalities

Annex 3. Interview guidance

Introduction

Questions

1. The current state (available data, data flows, mechanisms):

- What datasets are held by your organisation? (SCOPE)
- What are the legal mechanisms and organisational structures for data sharing? (STRUCTURE)
- Follow-up question: What are the responsibilities and roles in these mechanisms/structures as well as collaboration activities to deliver effective services?
- Follow-up question: Which legislation does your organization comply with? Is there any legislation in your policy domain specific to stakeholders regulated by your organization?
- How is the capacity for coherent implementation of data related activities (eg. technology, human resource capacity, data generation)? (CAPACITY)
- Follow-up question: How do you collect, process and store data?
- Follow-up question: What kind of big data analytics and business intelligence do you conduct?
- How does data flow between you and other organisations/stakeholders within country and across borders? (STAKEHOLDERS)
- Follow-up question: Who are the key stakeholders? (e.g. data stewards, data intermediaries (who facilitate access to data, e.g. groups that aggregate data), data users and/or decision-makers (e.g. government bodies, private sector, scientists, CSOs and/or individuals))
- Follow-up question: How do you collect data from stakeholders?
- Follow-up question: How is data currently shared in this topic area with stakeholders?
- How do you ensure data protection and privacy requirements (including with respect to personal and non-personal data)? (PROTECTION)

2. Challenges

- What are the challenges and/or blockers you see around access to data / flows and use of data?
  - Some examples:
    - These could be related to interoperability or particular types of data such as administrative/operational, transactional data, big data or open data or could exist across all data types, e.g. challenges around the mechanism (API, portal, etc) through which data is being shared, around parties' willingness to share data or around existing (or the lack of) data standards that would facilitate data sharing?
    - Needs for capacity development of the data-related skills and competencies such as data standards, data management, data analytics with a focus on administrative data and innovative (non-traditional) data sources and products, data security and privacy as well as data culture and data literacy?

3. Opportunities

- How could data sharing, data interoperability and data use be improved?
  - What data infrastructure and tools (including datasets, registers, standards, technology, policies and organisation) could help improve data sharing and use?
  - Follow-up question: Are new business models and possible mechanisms needed to support this infrastructure? If yes, how should they be designed?
  - Are there ongoing initiatives trying to solve challenges in this area? If yes, please mention them.
  - In your work, are any non-traditional data sources, such as telecommunication data or geospatial data, being used to inform requests that are coming in?

- Follow-up question: How can you use administrative data and innovative data sources including big data, Geospatial data, Citizen Generated Data (CGD)? Any plans or possibilities to enable linking of these data sources to integrate the methods?
- What are the possibilities to create partnership among the stakeholders for data sharing (e.g administrative data, private sector on big data and civil society organizations on CGD)?

4. Recommendations

- What recommendations can you make to develop and implement an efficient data governance framework?
- How do you (your institution) expect to benefit from the data governance framework? What will be your organization's efforts/contribution for implementation of data governance framework?

Outro/next steps

- Thank you, we really appreciate your time.
- Are there other contacts we should speak to?
- We will keep you updated about the progress and would love to continue to hear your feedback as we move along.

Annex 4. Definitions of some data terms

Term	Definition[170]
Data altruism	Data altruism is about individuals and companies giving their consent to make available data that they generate – voluntarily and without reward – to be used in the public interest. Such data has enormous potential to advance research and develop better products and services, including in the fields of health, environment and mobility.
Data controllers	Data controllers are organisations or individuals authorised by laws or regulations to make decisions regarding granting access to or permitting shared use of data under their control, regardless of whether this data is collected, stored, processed or distributed by this organisation or individual or by a representative acting on their behalf.
Data economy	The term data economy refers to industry in which institutions, value creation chains, competition dynamics and consumer market behaviour change as a result of the growing use of digital technologies that generate big data.
Data ecosystems	Data ecosystems is a term that describes the various stakeholders, services and applications (software) that use and share data for economic or social purposes. These include stakeholders from industry, science, civil society and government. The term data ecosystem does not imply that data behaves in the manner of a traditional ecosystem as the term is used in the context of natural sciences. Rather, the data ecosystem is a data-based system with its own frequently innovative technical, organisational and regulatory structures.
Data governance	Data governance describes the framework conditions (laws, directives, standards, internal regulations) and organisational structures relating to the management (administration and use) of data in public authorities, companies and other entities.
Data infrastructure	Data infrastructure can be understood as an interconnected technical infrastructure consisting of components and services that facilitates access to data as well as its storage, exchange and use.
Data intermediaries	Data intermediaries are institutions which link up access to data with the use of data by other users. They act as mediators. Data intermediaries include institutions with trustee functions or marketplace functions as well as other methods of data mediation.
Data marketplaces	Data marketplaces are centralised or local systems that connect data supply with data demand. These marketplaces implement monetisation mechanisms, for example in the form of subscription models (such as access price plus volume-dependent pricing).
Data protection	Data protection concerns the protection of citizens' basic rights and freedoms in the context of data processing, In particular it relates to their informational self-determination and right to maintain a private sphere.
Data security	Data security describes the technical and organisational measures required to ensure that the level of protection provided is appropriate to the particular requirements for protection.
Data sovereignty	The term data sovereignty extends beyond the bounds of data protection law and focuses on the autonomy of data subjects and also of companies and their data. These actors, with technical resources and their own skills, are able to act independently to determine the fate of their data.
Data subject	The data subject is an individual who is identified in data or identifiable from data.
Data trustees	A data trustee can be tasked with developing and implementing standardised access to data for approved agencies. Data trustees also function as advisers for users and, depending on their specialist field, offer various services such as data management for the benefit of users. Data trustees may also assert interests and rights under data protection law for a variety of consumers. Data trustees fall under the umbrella of the more generic term of data intermediaries.

[170] The definitions are based on Germany Data Strategy of Federal German Government (2021), https://www.bundesregierung.de/breg-en/service/information-material-issued-by-the-federal-government/data-strategy-of-the-federal-german-government-1950612

United Nations Development Programme
One United Nations Plaza
New York, NY 10017
www.undp.org