6 Enabling a data-driven public sector

Chapter 6 presents and analyses the efforts of the government of Thailand to enable and govern a data-driven public sector. It reviews its data governance arrangements as a structural foundation and considers Thailand's current experience in leveraging data availability, access and sharing to unlock greater value in its service design and delivery. Finally, it explores how better data governance from the perspective of ethics, privacy, transparency and security could help in reinforcing citizens' trust in relation to the use of data by the government.

Introduction

A data-driven public sector transforms the design and delivery of public policies and services through the strategic management, sharing and use of data (OECD, 2019[1]). To build a data-driven public sector, governments should recognise and demonstrate the potential of data to generate enormous insights to improve policy making, service design and delivery, and public sector outcomes for the ultimate benefit of citizens and businesses (OECD, 2019, p. 17[1]). With the COVID-19 pandemic, the need for governments to be digitally enabled and data-driven has become more urgent as it proved to boost the country's resilience, management of the crisis and social and economic continuity.

Pivotal to achieving this is strong data governance, which, as a core system of the public administration, enables coherent decision making and implementation, accountability and transparency. It ensures that the tools, measures and mechanisms used to generate public value from the data are framed by elements of trust and integrity, such as ethics, privacy, transparency and security.

As the level of understanding and acknowledgement by governments of data as vital resources for public value increases, efforts have been directed towards bridging legacy systems, organisational, operational and infrastructure silos to enable the establishment of a data-driven public sector. The path to becoming a data-driven public sector is not evident and easy. It involves creating an enabling environment for the access, sharing and use of data to spark innovation and opportunities for public sector, economic and social development, while raising transparency and accountability from the government. Converting data into tangible, measurable and consistent public value outcomes remains elusive, especially when facing risks of data misuse and abuse by businesses and governments.

Building blocks for a data-driven public sector

In the drive towards fostering more open, digital and innovative governments, the OECD has identified the creation of a data-driven public sector as a chief condition for successful digital transformation. Principle 3 of the OECD *Recommendation of the Council on Digital Government Strategies* (2014, p. 7[2]) informs of the need to create a data-driven culture in the public sector by developing frameworks that guide the access and re-use of data and deliver trustworthy official data in open formats (Box 6.1).

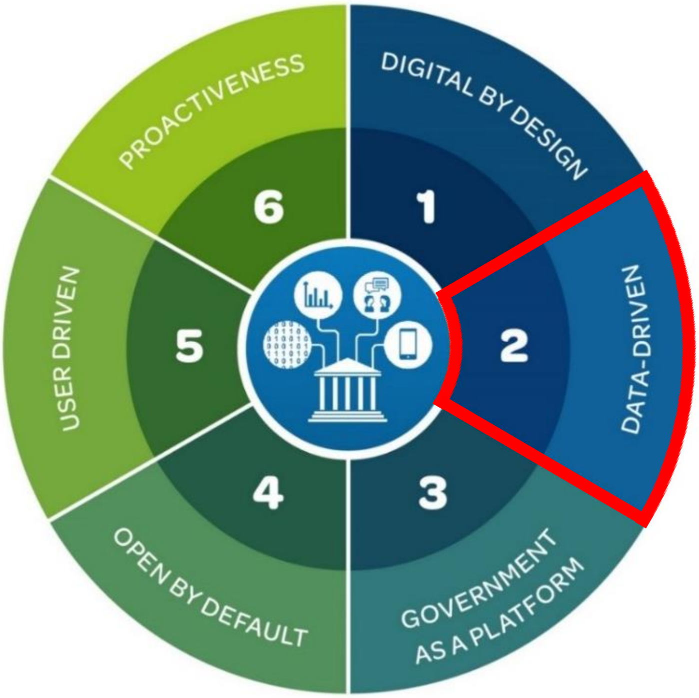
Box 6.1. OECD *Recommendation of the Council on Digital Government Strategies*: Principles 3

> *"The [OECD] Council [...] on the proposal of the Public Governance Committee [...] recommends that governments develop and implement digital government strategies which:*
>
> *Create a data-driven culture in the public sector, by:*
>
> *Developing frameworks to enable, guide and foster access to, use and re-use of the increasing amount of evidence, statistics and data concerning operations, processes and results to: (a) increase openness and transparency; and (b) incentivise public engagement in policy making, public value creation, service design and delivery.*
>
> *Balancing the need to provide timely official data with the need to deliver trustworthy data, managing risks of data misuse related to the increased availability of data in open formats (i.e. allowing use and re-use, and the possibility for non-governmental actors to re-use and supplement data with a view to maximise public economic and social value)."*

Source: OECD (2014[2]), *Recommendation of the Council on Digital Government Strategies*, https://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf.

In line with the above, the OECD Digital Government Policy Framework highlights the data-driven public sector as one of its core six dimensions (Figure 6.1). In a data-driven public sector, governments are able to apply data for designing policies, public services and long-term plans, generating public value to meet the changing needs and higher expectations of citizens and businesses (OECD, 2019[1]). It implies engaging in active efforts to remove barriers to the use of data, publishing public sector data freely and openly, encouraging the use or sharing of data among public sector organisations while protecting the data rights of citizens and businesses (OECD, 2019, p. 17[1]).

Figure 6.1. The OECD Digital Government Policy Framework: Data-driven public sector dimension



Source: OECD (2020[3]), "The OECD Digital Government Policy Framework: Six dimensions of a Digital Government", https://doi.org/10.1787/f64fed2a-en.

The opportunities of a data-driven public sector can be classified into three main pillars where data-driven initiatives can support the decision-making process across different policy areas and levels of government (Table 6.1):

- **Anticipatory governance**: Use data to strengthen a data-driven public sector’s anticipatory capacities and future-oriented approaches.
- **Design and delivery**: Engage stakeholders in policy making and the development of public services that respond to the needs of the users at any given point in time.
- **Performance management**: Enhance the monitoring, management and improvement of performance.

Table 6.1. Opportunities of a data-driven public sector

Anticipatory governance	Design and delivery	Performance management
Forecasting to proactively identify developments and future needs.	Engaging with citizens and businesses and co-value creators.	Acquiring resources effectively and using resources efficiently.
Foresight to prepare for multiple plausible alternative outcomes.	Predicting and responding better to citizens' and businesses' needs.	Attaining a higher quality and evaluation of performance.

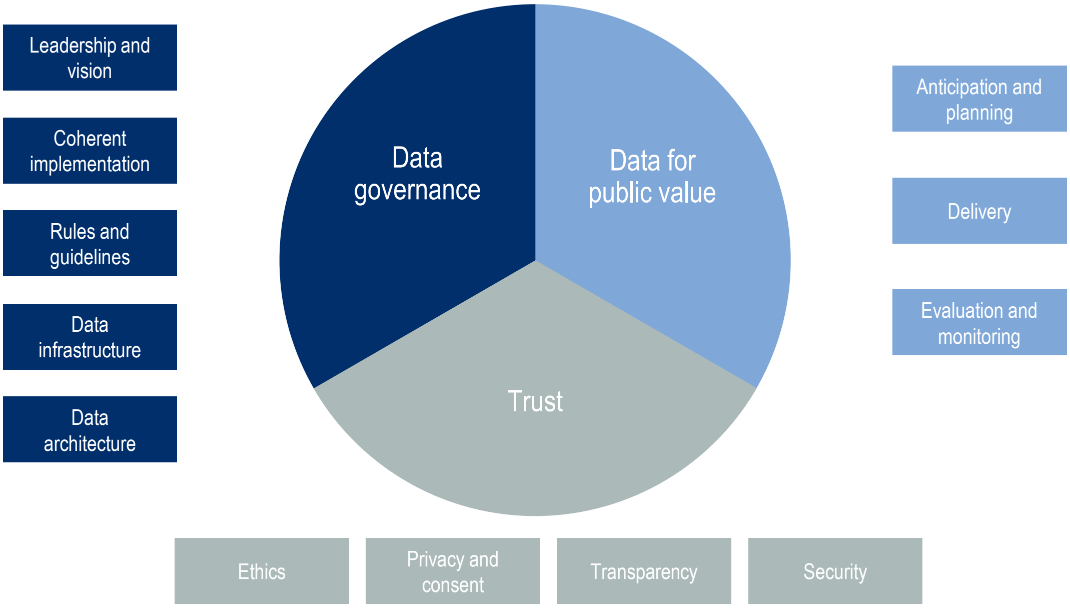
Source: Adapted from van Ooijen, C., B. Ubaldi and B. Welby (2019[4]), "A data-driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance", https://dx.doi.org/10.1787/09ab162c-en.

Analysing Thailand's efforts to enable a data-driven public sector

Building a data-driven public sector is not an easy task. Indeed, results from the OECD Digital Government Index show how the data-driven public sector is the second-lowest dimension of all of the six dimensions assessed in the OECD Digital Government Policy Framework. These results show that "governments are not yet fully exploiting the potential of data as a foundation for digital government and should foster the creation of a skilled public sector that relies on data as a core component to effectively design and deliver projects" (OECD, 2020[5]).

For the government of Thailand to reach digital government maturity and build a data-driven public sector with a whole-of-government approach, there are three key areas for discussion and consideration that will be covered in the three sections of this chapter: i) strengthening **data governance** arrangements as the structural foundation, which establishes how authority, control and decision making over data assets are carried out (Ladley, 2012[6]); ii) leveraging data access and sharing to increase **public value** in service design and delivery; and iii) establishing the role of data governance for **trust** in governments. The structure is also based on the OECD's analytical framework that holistically accounts for a data-driven public sector, featuring 12 facets with 3 areas of focus needed to successfully unlock the value of data (Figure 6.2).

Figure 6.2. The OECD analytical framework for a data-driven public sector



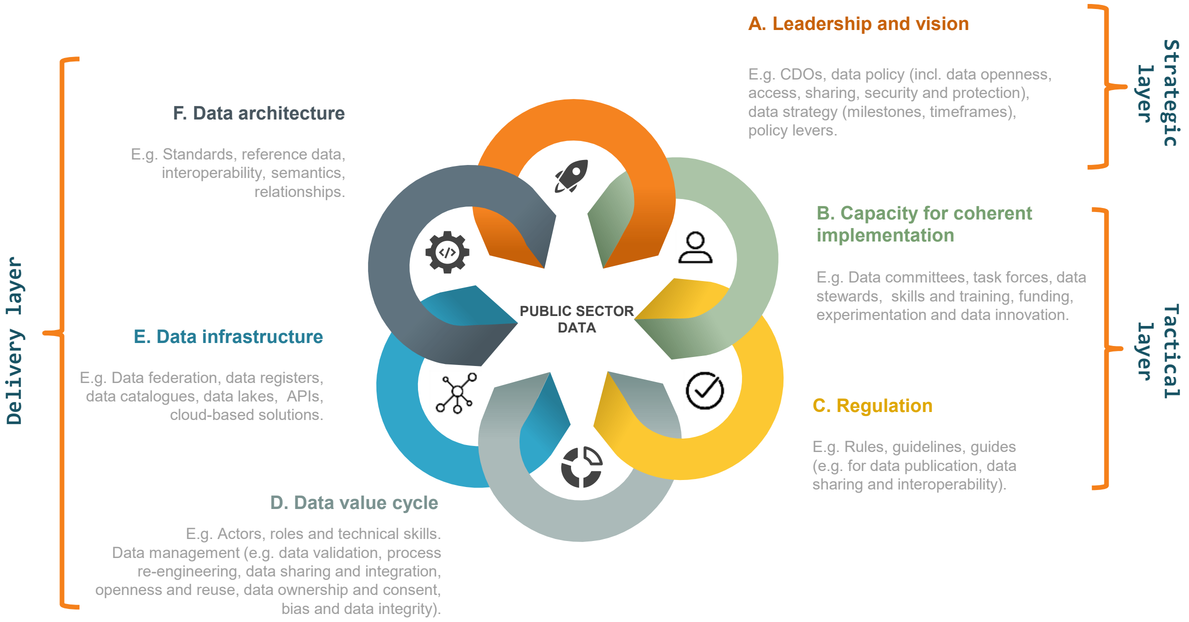
Source: OECD (2019[1]), *The Path to Becoming a Data-Driven Public Sector*, https://doi.org/10.17878/059814a7-en.

Strengthening public sector data governance in Thailand

Building a data-driven public sector implies strengthening the leadership, co-ordination, and regulatory, institutional and technical facets of data governance (Figure 6.3). These facets are structural and therefore fundamental to build the basis for the trustworthy and enhanced access to sharing and use of data by public entities. The six facets are organised into three different layers: the strategic layer (leadership and vision), the tactical layer (capacity for coherent implementation and regulation) and the delivery layer (data value cycle, data architecture, data infrastructure).

As such, this first section on "Strengthening public sector data governance" will focus on the aspects of leadership, power and capacity for co-ordination, strategy, management and regulation, in line with the data governance strategic and tactical layers presented in Figure 6.3.

Figure 6.3. The OECD model for data governance in the public sector


A. Leadership and vision
E.g. CDOs, data policy (incl. data openness, access, sharing, security and protection), data strategy (milestones, timeframes), policy levers.
Strategic layer
F. Data architecture
E.g. Standards, reference data, interoperability, semantics, relationships.
B. Capacity for coherent implementation
E.g. Data committees, task forces, data stewards, skills and training, funding, experimentation and data innovation.
Delivery layer
PUBLIC SECTOR DATA
E. Data infrastructure
E.g. Data federation, data registers, data catalogues, data lakes, APIs, cloud-based solutions.
Tactical layer
C. Regulation
E.g. Rules, guidelines, guides (e.g. for data publication, data sharing and interoperability).
D. Data value cycle
E.g. Actors, roles and technical skills. Data management (e.g. data validation, process re-engineering, data sharing and integration, openness and reuse, data ownership and consent, bias and data integrity).

Source: OECD (2019[1]), *The Path to Becoming a Data-Driven Public Sector*, https://doi.org/10.1787/059814a7-en.

The government of Thailand is not oblivious to the importance of data governance in the public sector – a vision which is shared by leading OECD member countries in this field such as Estonia, New Zealand and Norway (OECD, 2019, p. 30[1]).

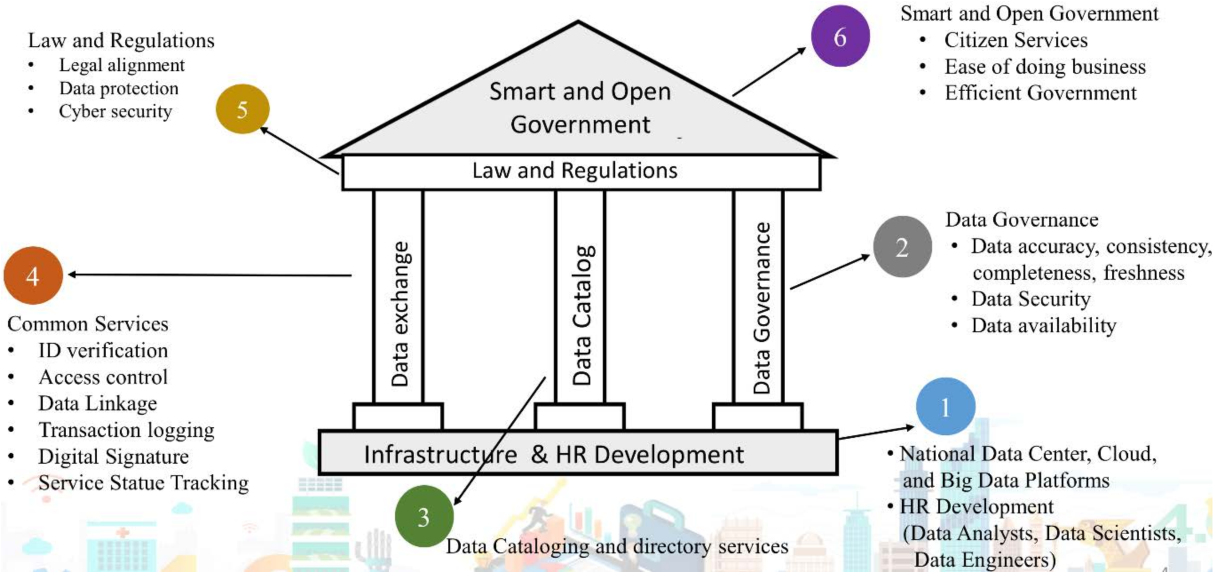
In the past few years, the government of Thailand has made efforts to provide formal ministerial support and establish governance structures for Thailand's initial phase of the transition to a data-driven public sector. The Digital Government Development Agency (DGA) developed the Data Governance Framework 1.0 in 2018, which emphasises the importance of governing data to support the development of Thailand's digital economy and society but also highlights the challenges it faces, namely data duplication, data quality, data security and information disclosure (DGA, 2018, p. 10[7]).

Yet, while there is ambition in Thailand to build a digitally enabled and data-driven public sector, the digital foundations built from 2018 are still not sufficiently robust and need to be further strengthened. For instance, as part of its research work, the DGA has expressed a lack of clear direction and comprehensive measures and guidelines on the management and supervision of public data (DGA, 2018, p. 10[7]).

Under the Data Governance Framework, the DGA defines data governance as a mechanism for determining the direction, control and verification of the management of data, such that the data are secure, of quality, cost-effective and economically and socially valuable, and the acquisition and use of government information are accurate, complete, current, safe and private (DGA, 2018, p. 10[7]). It establishes the rights, duties and responsibilities of every stakeholder and defines the policies and standards for creating, using and managing data such as the data value cycle, quality of information and metadata (DGA, 2018, pp. 13-14[7]). The standards within the Data Governance Framework 1.0 aim to support every government agency in building the foundations to work towards digitalisation from the processing to the collection, distribution and exchange of data.

When compared to the OECD data governance model for the public sector presented in Figure 6.3, most of these elements fit in the delivery aspects of data governance (e.g. data quality, metadata) while others are more tactical (e.g. roles and responsibilities). Additionally, the Thai Government Data Service Framework (Figure 6.4) expresses clearly how the most technical and delivery aspects of data governance are foundational pillars for the construction of a smart and open government.

Figure 6.4. Thailand's Government Data Service Framework



Source: NSO (2019[8]), "Big data application in Thailand's government", https://unstats.un.org/bigdata/events/2019/hangzhou/presentations/day3/5.%20Big%20Data%20Application%20in%20Thailand%E2%80%99s%20Government.pdf.

Leadership

Political and administrative leadership are crucial to secure the success of Thailand's willingness to use data both in the design and implementation of public policies and services. Political leadership involves high-level support from ministers to advance the policy agenda, while administrative leadership are of top management positions in the public sector that focus on steering policy design and implementation, which helps to ensure continuity across political terms (OECD, 2019, p. 39[1]). Power derives from this leadership to a large extent but is also dependent on a host of other factors, such as the institutional position in the hierarchy, defined roles and responsibilities and their legal basis, and the policy levers that leaders and public sector organisations use to steer policy and enforce compliance (e.g. of data standards).

As discussed in Chapter 2, the Ministry of Digital Economy and Society (MDES) is the public sector organisation that takes the greatest lead on the national digital (government) and data agenda: Thailand's

National Big Data Policy and Digital Government Development Plans (further elaborated in the next sub-section "Towards an action plan for public sector data").

The MDES, together with the Digital Government Development Commission and the DGA, leads the development of data governance and policies as part of the National Big Data Policy and Digital Government Development Plans.

On the one hand, the Digital Government Development Commission was created in 2019 under the promulgation of the Digitalisation of Public Administration and Services Delivery Act, B.E. 2562 (2019). It has significant political and administrative power, as it brings together the prime minister of Thailand as the chairperson, and the Minister of Digital Economy and Society, the Permanent Secretary of the MDES, the Permanent Secretary of the Office of the Prime Minister (PMO), the Permanent Secretary of the Ministry of Higher Education, Science, Research and Innovation (MHESI), the Secretary-General of the Office of the Civil Service Commission (OCSC), the Secretary-General of the Office of the Public Sector Development Commission (OPDC), the Secretary-General of the Office of the National Economic and Social Development Council (NESDC) and the Director of the Budget Bureau as the members. Other members are selected from the National Digital Economy and Society Commission, the Electronics Transactions Commission, the Office of the Official Information Commission, the Personal Data Protection Commission and the National Cyber Security Commission.

The Digital Government Development Commission has powers and duties to provide guidance and recommend policies to government agencies and formulate the Digital Government Development Plans and its roadmaps, principles, standards, rules, regulations and guidelines, especially in data governance. The commission is required to track and monitor the progress of digital government in Thailand (Box 6.2). Additionally, the DGA and the commission also provide policy recommendations to the cabinet on digital government development. In that regard, the Office of the Permanent Secretary and the PMO have been keen in co-operating with the DGA and its governing commission to support the implementation of the Digital Government Development Plan.

Box 6.2. Digitalisation of Public Administration and Services Delivery Act, B.E. 2562 (2019) – Specific provisions on data governance

> *"**Section 7***
>
> *The Digital Government Development Commission shall have the following duties and powers:*
>
> *[…]*
>
> *(2) To specify the principle of governmental data governance as a foundation and guideline to ensure compliance with this Act; […].*
>
> ***Section 8***
>
> *The governmental data governance under Section 7(2) shall, at least, consist of the following:*
>
> *(1) The determination of rights, duties and responsibilities in the management of data of State Agencies, including the right and duties of the person possessing or controlling the data in every step throughout the procedure;*
>
> *(2) There being an administration system and a comprehensive procedure for data management and protection which covers the production, storage, categorisation, processing or use, classification or disclosure, inspection, and destruction;*
>
> *(3) There being a measure to control and improve data quality for the purpose of ensuring that the data is correct, comprehensive, readily available, up-to-date, integrable and can be shared, including there being*

> *an evaluation on the data management in order for State Agencies to have quality data, and to be able to develop their innovation using such data;*
>
> *(4) The determination of clear and systematised policies or rules on access and utilisation of data, including measures and guarantees for the protection of possessed data to ensure security and prevent privacy violation;*
>
> *(5) The production of the data catalogue on the government's digital metadata in order to expound on the data structure, content, form of storage, sources and right to access the data."*

Source: Information provided to the OECD by the Thai government.

On the other hand, the DGA delivers policy recommendations on digital government transformation, data governance and digitalisation of public services backed by political support. The DGA's role in building a data-driven public sector is set out in B.E. 2561 (2018), a royal decree that established the DGA under the supervision of the prime minister and the PMO. The government-to-government (G2G), government-to-citizen (G2C) and government-to-business (G2B) initiatives of the DGA are issued either as prime minister's orders or cabinet resolutions (DGA, 2018, p. 33[9]). Moreover, the Digitalisation of Public Administration and Services Delivery Act, BE. 2562 (2019), specifically states that the DGA has "the duty of directing and facilitating the operations as assigned by the Digital Government Development Commission, including its secretarial and academic works". In this sense, the DGA has a similar scope to the Digital Government Development Commission.

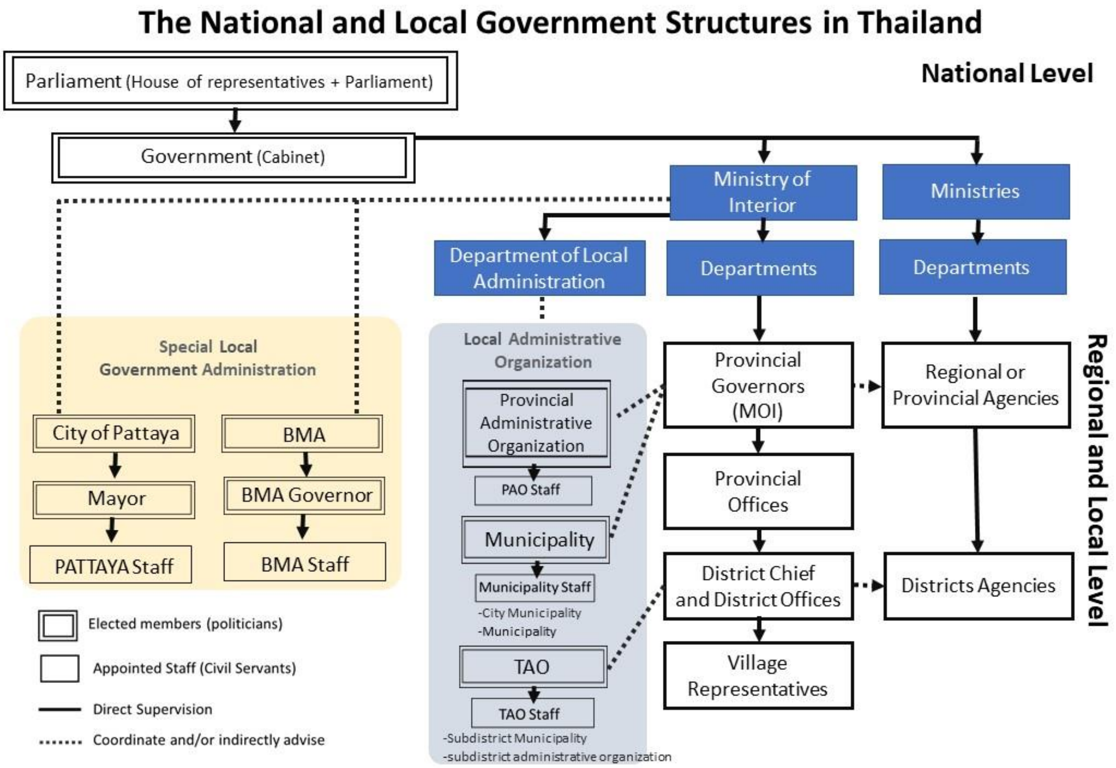
However, the DGA fares less on administrative power in the implementation of the digital government and data agenda. The DGA, as the key public sector organisation that promotes and supports the rolling out of digital government services, does not play a strong co-ordination and compliance role for data governance across the public sector. Broadly, the MDES and DGA co-ordinate with other ministries and government agencies on different mandates under the 20-Year Digital Economy and Society Development Plan (2017-2036) or Digital Thailand, one of which includes the move to big data as discussed in Chapter 2.

The DGA's limited administrative power is evident in the less-than-optimal results in data management and integration at an operational level. In 2018, the DGA conducted a "Survey Project on the Readiness of Digital Government Development of Government Agencies in Thailand" in line with the Digital Government Readiness Assessment Framework, B.E. 2561 (2018). Two dimensions, "Policies/practices" and "Secure and efficient infrastructure", measured the development readiness of government agencies on data governance and data management respectively.

On a scale of 0 to 100 points (with 100 being the most prepared), the survey revealed that the average readiness of 287 public sector organisations at the department level surveyed was 52.7 points for "Policies/practices" and 75.2 for "Secure and efficient infrastructure"; 1 237 public sector organisations at the provincial level surveyed had 33.9 points for "Policies/practices" and 54.6 points for "Secure and efficient infrastructure" (DGA, 2018, pp. 47-49[9]). These capacity and capability limitations do not only bring data governance challenges at the central level, they translate into multi-level data governance issues, in particular when specific data is generated by local public sector organisations but consumed by central authorities as an input for policy and decision making.

Previous efforts to build multi-level data governance arrangements for effective policy making have not been entirely successful in moving forward due to the disparities in terms of data capacities, protective data management practices at the local levels and the complex multi-level governance arrangements and accountability mechanisms among local, provincial and central authorities (Figure 6.5).

Figure 6.5. Thailand's national and local government structure


The National and Local Government Structures in Thailand
National Level
Parliament (House of representatives + Parliament)
Government (Cabinet)
Ministry of Interior
Ministries
Department of Local Administration
Departments
Departments
Special Local Government Administration
City of Pattaya
BMA
Mayor
BMA Governor
PATTAYA Staff
BMA Staff
Local Administrative Organization
Provincial Administrative Organization
PAO Staff
Municipality
Municipality Staff
-City Municipality
-Municipality
TAO
TAO Staff
-Subdistrict Municipality
-subdistrict administrative organization
Provincial Governors (MOI)
Regional or Provincial Agencies
Provincial Offices
District Chief and District Offices
Districts Agencies
Village Representatives
Regional and Local Level
Elected members (politicians)
Appointed Staff (Civil Servants)
Direct Supervision
Coordinate and/or indirectly advise

Source: Information provided to the OECD by the Thai government.

In reference to the DGA's organisational key objectives (Box 6.3), the DGA should strengthen the first and second key objectives as top priorities: in devising, executing and enforcing the implementation of its G2G (including central-local data exchange), G2C and G2B initiatives at the operational level for national, department and provincial public sector organisations. The other key objectives are oriented more towards having DGA play a supporting role in promoting digital government transformation. Imparting greater authority to the DGA as the leading public sector organisation that reports directly to the Digital Government Development Commission could help to attain better co-ordination on digital and data standards, digital and data infrastructure and digital services that rely on data as an important input.

Box 6.3 Thailand's Digital Government Development Agency (DGA): Key objectives

- Reinforce, administrate and provide digital technology infrastructure services and service systems or fundamental applications engaging with digital government.
- Implement standards, models, measures, principles and approaches in the form of digital technology as well as the transactional process in order to bridge information and work systems among government agencies legitimately and concordantly.
- Promote and endorse the integration and exchange of information among government agencies, the disclosure of government information through digital technology and set out government information sharing centres to facilitate the provision of services to people and government agencies' transactional processes.
- Enhance and ratify government agencies to provide digital services to concerned parties.

- Reinforce a one-stop government digital service which people can access conveniently, promptly and securely.
- Advocate and promote government agencies in terms of the project management and administration of digital technology as well as endorse, sponsor and impart academic services and training in order to optimise government officers' digital competencies.
- Study, research, experiment, endorse and sponsor academic works, research and innovations to enhance digital government development.
- Promote government transactions that are accountable for the annual budget allocation framework involving digital government as well as fortify the monitoring and evaluation of digital government transactions and plans.
- Proceed with other matters with regard to digital government developments as per the law and cabinet orders.

Source: DGA (2018[9]), *Annual Report 2018*, https://www.dga.or.th/upload/editor-pic/files/AR_ENG_DGA-2018.pdf.

This would require the political and administrative leadership at the MDES, PMO, MHESI, OCSC, OPDC, NESDC, etc. to confer a higher degree of power and authority to the DGA, such that the DGA has greater oversight beyond its advisory role in the context of the National Big Data Policy and data policies under the Digital Government Development Plans. This is to secure good data governance as the foundation towards data integration and sharing, with the publication of good quality open government data – and how this can be done will be covered in the following sub-sections on "Towards an action plan for public sector data" and "Capacity for coherent implementation".

A positive development to illustrate this point is that the DGA currently supports the new Digital Government Development Plan (2020-2022) in drafting more standards and guidelines. Based on this plan, the Data Catalogue Guidelines on Mandatory Metadata for Agency Data Catalogues will be defined in 2021, which will lead to the development of the Thailand Government Data Catalogue that assimilates all government agency data catalogues, under the supervision of the MDES National Statistical Office of Thailand (NSO). In 2020, the DGA identified the flagship project on the Agency Data Catalogue and worked with the OPDC to encourage a pilot project on government data.

Clear identification of the DGA as the key public sector organisation that will officially lead, co-ordinate, implement and ensure compliance with data governance by decree would be helpful to increase its power and authority. While the current leading role of the MDES is inclusive and relevant, there is a risk that public sector data initiatives under the National Big Data Policy and Digital Government Development Plans will not be granted enough political and administrative support *vis-à-vis* other digital economy policy goals (see next sub-section on "Towards an action plan for public sector data").

While the MDES could continue to maintain oversight, provide an overarching direction and play a wider advisory and co-ordination role for the National Big Data Policy and Digital Government Development Plans, it would be critical for the leading role of the DGA to be confirmed beyond its current operational focus and de facto role as a provider of technology solutions for the public sector.

On top of institutional leadership, the identification of personal leadership is another core element of good data governance. Well-defined roles and responsibilities of key positions help to cement the power and authority of the leading public sector organisation for the national data agenda. The President and Chief Executive Officer (CEO) of the DGA could formally be the National Chief Data Officer (CDO) or Chief Information Officer (CIO) of Thailand, who administratively leads the digital government and data policy in the country.

This is done in New Zealand, where the government's Chief Data Steward is also the Chief Executive of Statistics and is in charge of providing direction on the national data policy. There are clear quarterly key deliverables for this data leadership role (OECD, 2019, p. 39[1]). Similarly, in France, the General Data Administrator is attached to the Head of Etalab, the taskforce within the PMO in charge of co-ordinating open data and artificial intelligence (AI) policy (OECD, 2019, p. 39[1]). The actual title can differ from country to country but what the government of Thailand most needs is a formal leadership position and role with enough political support and administrative power, supported by well-defined performance indicators and a vision in terms of outcomes for the national data agenda and data governance policy.

Towards an action plan for public sector data

A comprehensive and sustainable strategy that is aligned with policy objectives and priorities is a crucial policy instrument to achieving the desired data-driven public sector. National data strategies and action plans require a high-level, deliberate approach and political commitment towards the role of data as a strategic resource, to unlock economic and social value in line with other policy goals while managing and mitigating risks associated with data use (OECD, 2019, p. 1[10]). Based on front-running countries' practices in this area, the OECD has found that national data strategies and action plans are often placed within broader digitalisation plans.

Thailand's national data strategy is contained in its National Big Data Policy, which is led by the MDES and the DGA (Box 6.4). Under the MDES, the Office of the National Digital Economy and Society Commission (ONDE) has the mandate for drafting national policies on digital economy and society for the National Digital Economy and Society Committee and co-ordinating with the Digital Economy Promotion Agency (DEPA) (ONDE, 2020[11]). According to the ONDE, one of its main objectives is to ensure that big data generates economic and social value by improving operational efficiency in production and services (ONDE/MDES, 2019[12]). As such, the National Big Data Policy is placed within the broader national digitalisation plans for the government, economy and society and framed in the context of the larger 20-Year Digital Economy and Society Development Plan (2017-2036) or Digital Thailand. Furthermore, big data is treated as the architectural foundation on which other data initiatives and innovations are built such as open government data, digital government services and more broadly, digital businesses and innovations (ONDE/MDES, 2019[12]).

Box 6.4. Thailand's National Big Data Policy

In mid-2017, Thailand's prime minister General Prayuth Chan-o-cha and the cabinet started work on the National Big Data Policy. The key public sector institutions driving this policy are the MDES and the DGA. The initial goals were to manage big data within the public sector and enhance the efficiency of the government's one-stop service. In this initial stage, the Government Data Centre and Cloud Service (GDCC) was established to enable the centralisation of a secured computer network service for the public sector and promote basic knowledge on cloud computing among public officials.

Recently in 2019, the Government Big Data Institute (GBDi) was established under the DEPA to respond to the needs of promoting the effective use of big data and enable public officials to develop skills in big data analytics for their respective government agencies. The ultimate objective of setting up the GBDi is to foster data-driven decision making and operational insights for public sector organisations, such that they can respond to the needs of citizens through public services delivery effectively.

In line with the establishment of the GBDi and DEPA, the prime minister and the cabinet also set a target for all public sector organisations to massively integrate data for use by the end of 2017. The MDES and DGA were tasked to collect data and insights on how to maximise the use of big data from different public sector organisations and become data-driven.

The initial projects related to the utilisation of government big data include:

1. Data integration from the National Statistics Office, Ministry of Public Health, Ministry of Justice and Ministry of Social Development and Human Security to analyse schemes to help low-income individuals.
2. Data integration from the Hydroinformatics Institute to develop a Water Situation Map to forecast and monitor potential droughts and floods.
3. Data integration from the Ministry of Public Health to create a Health Data Centre that analyses trends and offers statistics on hospital traffic throughout the country.

Source: Information provided to the OECD by the Thai government.

Thailand's National Big Data Policy can be made more coherent and sustainable by further clarifying its role, positioning and scope as a meta data governance instrument (i.e. a policy governing policies) that addresses data policy issues related to different sectors. It would be helpful for the National Big Data Policy to have specific and dedicated data strategies and actions plans addressed to each sector. The demarcation of the purposes, corresponding actions and intended outcomes for specific public sector organisations or segments need to be clear. This implies reinforcing the relevance of those areas that fall directly under the government sphere (i.e. open government data, data ethics in the public sector).

Ireland, the Netherlands and the United States (US) have done this comprehensively in their national data strategies and action plans. Ireland's Public Service Data Strategy (2019-2023) is clear in linking its overall national data strategy with other data initiatives and policy instruments such as the National Data Infrastructure and Open Data Strategy, thereby establishing a unified and cohesive approach to implementing public sector data initiatives with shared principles, objectives and actions (OECD, 2019, p. 38[1]). The Netherlands' Government Data Agenda, which focuses on unlocking the value of data as a tool to address policy challenges, integrates the country's policy goals with improved management of data in the public sector, and publication and re-use of open government data. Moreover, the implementation of this agenda is the shared responsibility of the Dutch Ministry of the Interior and Kingdom Relations, central and local governments (OECD, 2019, p. 37[1]). The US Federal Data Strategy and 2020 Action Plan consists of detailed principles, practices and steps to take to leverage the value of data for the whole federal government data asset portfolio (Box 6.5).

Box 6.5. The US Federal Data Strategy and 2020 Action Plan

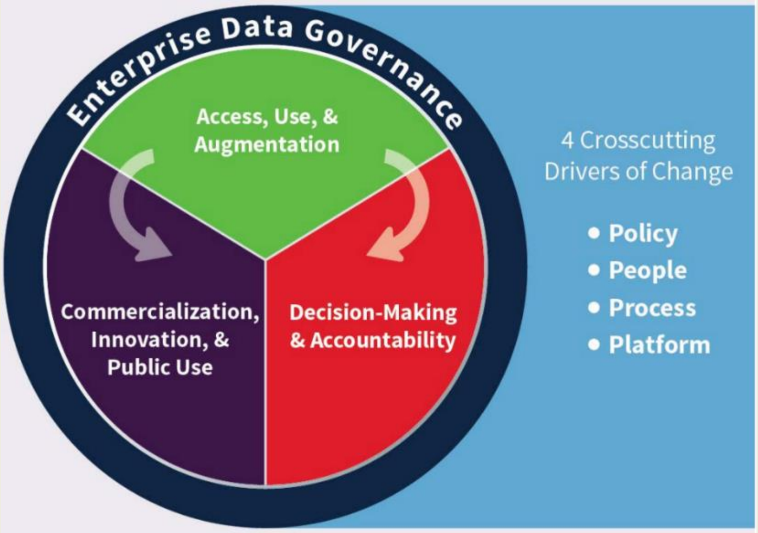
The US Federal Data Strategy

In June 2019, the US government issued its Federal Data Strategy, which presents a ten-year vision to unlock the full potential of the country's federal data assets while safeguarding security, privacy and confidentiality. It adds to several existing initiatives, policies, executive orders and laws that over the past few decades have helped make the US a front-runner in terms of strategic management and re-use of government data. The Federal Data Strategy is based on three core principles: ethical governance, conscious design and learning culture.

In order to capture the linkage between user needs and appropriate management of data resources, the data strategy covers 40 practices that guide agencies throughout their adoption of the strategy. To further ensure coherent implementation of the strategy in the early phase, federal agencies are required to adhere to annual government action plans that include prioritised steps, time frames and responsible entities. The Federal Data Strategy focuses on four areas:

- **Enterprise data governance**: Focuses on the management of government data. Establishes data policies and specifies the roles and responsibilities for public sector organisations regarding data privacy, security and confidentiality protection. Defines the roles and responsibilities for monitoring compliance with data standards and policies.
- **Access, use and augmentation**: Focus on the development of policies and procedures to ensure public sector organisations and external stakeholders can easily access and re-use government data – through improving data dissemination, increasing the amount of non-sensitive data available on line and leveraging new technologies and best practices to promote access to sensitive or restricted data while protecting the rights of citizens.
- **Decision making and accountability**: Aim to improve the use of data for decision making and accountability purposes and promote the use of data for policy monitoring and evaluation purposes to inform future policy decisions. Focus on the provision of high-quality and timely data for evidence-based decision making or on providing specific datasets such as spending data to foster public sector accountability and transparency.
- **Commercialisation, innovation and public use**: Focus on facilitating the use of government data by external stakeholders, making the data more accessible and relevant for commercial purposes, innovation or other public uses. Foster the use of government data to promote economic, good governance and social value, targeting different groups such as private firms, researchers or citizens.

Figure 6.6. Four focus areas of the US Federal Data Strategy


Enterprise Data Governance
Access, Use, & Augmentation
Commercialization, Innovation, & Public Use
Decision-Making & Accountability
4 Crosscutting Drivers of Change
• Policy
• People
• Process
• Platform

US 2020 Action Plan

The 2020 Action Plan establishes a solid foundation that will support the implementation of the Federal Data Strategy over the next decade until 2030. It identifies initial actions for agencies that are essential for establishing processes, building capacity and aligning existing efforts to better leverage data as strategic assets. It also covers 16 critical steps to launch the first phase of the data strategy vision, including the development of data ethics frameworks and data science training for federal employees. Furthermore, it encompasses a series of pilot projects underway at various government agencies and a set of government-wide efforts designed to support all agencies through the development of tools and resources. Finally, Annual Action Plans are developed iteratively and incorporate stakeholder feedback and input.

Source: US Government (2020[13]), *2020 Action Plan*, https://strategy.data.gov/action-plan/.

Developing a comprehensive national data plan covering the central, subnational and local levels would be critical for enabling an extensive data-driven public sector for Thailand. As with the Digital Government Development Plans, the DGA, together with the Digital Government Development Commission, could take the lead in developing an Action Plan for Public Sector Data or a similar policy document, which not only aligns to future National Economic and Social Development Plans and Digital Government Development Plans but also connects and underlines the different data policy aspects discussed earlier (e.g. open government data, data ethics). Moreover, this Action Plan for Public Sector Data should be acknowledged as a core element of the National Big Data Policy to further clarify the value of the latter as a metadata governance instrument as mentioned earlier.

In addition, the government of Thailand fares well in providing strong political support and will to create and see through its National Big Data Policy but falls short on the operational aspect for the execution and implementation of the National Big Data Policy, in particular addressing data access, sharing and re-use in the public sector. Therefore, the Action Plan for Public Sector Data should also set the right accountability and enforcement mechanisms supported by a stronger lead role of the DGA as proposed earlier. As such, it will need to specify targets, monitoring mechanisms and impact assessments for each key stakeholder and milestone.

A way to move forward in the short term could involve an inclusive approach for the development of the Action Plan for Public Sector Data in consultation with the wider digital government ecosystem of the public sector, private sector and civil society stakeholders. For instance, the United Kingdom (UK) had employed an open consultation process for its National Data Strategy, with the Department for Digital, Culture, Media and Sport collecting evidence from the public that could inform the development of the strategy and conducting a series of roundtables and testing exercises in view of the final document in 2020 (OECD, 2019, p. 38[1]). Another example is that of Germany, which conducted several public consultation rounds with an expert committee and a broad-based online process with citizens and specialists on a draft paper for a national data strategy promoting data provision, access, sharing and responsible data use before the final Data Strategy of the Federal Government was presented in mid-2020 (Die Bundesregierung, 2020[14]).

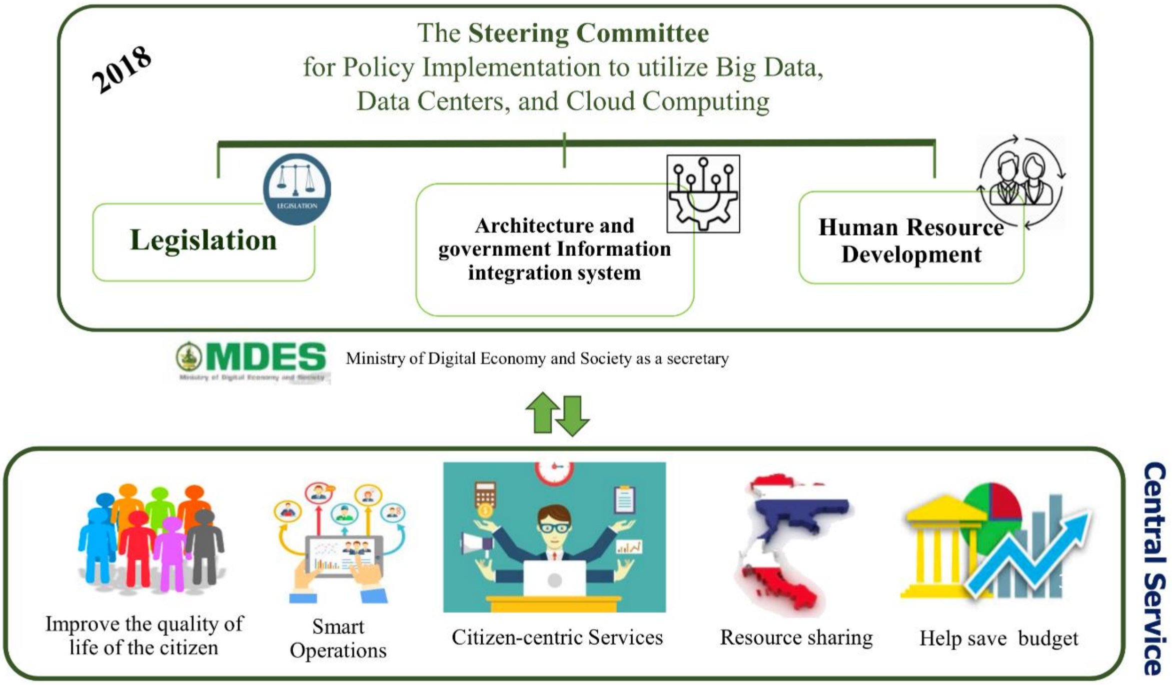
Such an open, inclusive and collective approach is especially important with the government of Thailand's vision to integrate systems, data and information from over 400 government agencies and consolidate their public services into a one-stop digital government platform for citizens and businesses to access conveniently, promptly and securely, as shared during the OECD peer review mission in Bangkok. Moreover, this approach could help in building ownership within the public sector – beyond the identification of those gaps as done by the DGA through the Survey Project on the Readiness of Digital Government Development of Government Agencies in Thailand.

Capacity for coherent implementation

Institutional co-ordination and compliance

The MDES co-ordinates the National Big Data Policy through the Steering Committee for Big Data, Data Centres and Cloud Computing (Figure 6.7), with the former acting as secretary. This secures the MDES' leadership, decision-making and co-ordinating role, with the political backing of the deputy prime minister as chairperson and the Minister of Digital Economy and Society as vice-chairperson (Tortermvasana, 2018[15]). The composition of the steering committee involves 20 line ministries that carry out projects in diverse line and horizontal policy areas like agriculture, tourism, taxation, mobility and natural resources (NSO, 2019[8]). The committee members are the permanent secretaries of the 20 ministries, the NESDC and the DGA.

Figure 6.7. Thailand's Steering Committee for Big Data, Data Centres and Cloud Computing


2018
The Steering Committee
for Policy Implementation to utilize Big Data,
Data Centers, and Cloud Computing
Legislation
LEGISLATION
Architecture and government Information integration system
Human Resource Development
MDES
Ministry of Digital Economy and Society
Ministry of Digital Economy and Society as a secretary
Improve the quality of life of the citizen
Smart Operations
Citizen-centric Services
Resource sharing
Help save budget
Central Service

Source: NSO (2019[8]), "Big data application in Thailand's government", https://unstats.un.org/bigdata/events/2019/hangzhou/presentations/day3/5.%20Big%20Data%20Application%20in%20Thailand%E2%80%99s%20Government.pdf.

The Steering Committee for Big Data, Data Centres and Cloud Computing aims to steward the management of all of the data generated by the state agencies and inform policy and decision making for the digital transformation journey – by consolidating data from all ministries involved into a centralised big data management system. This process involves the conversion, identification and structuring of public value data to be generated across different policy areas: citizens' quality of life, smart operations, citizen-centric services, resource sharing and budgetary savings.

The committees under the steering committee undertake specific tasks such as data structuring and management in parallel with extracting knowledge and insights from the datasets and designing targeted strategies to improve public processes and service delivery. For this purpose, the committees are charged with fundamental tasks such as discovering, naming and verifying datasets, and identifying areas to generate public value – with the objective of creating an ecosystem to facilitate policy and business decisions (Tortermvasana, 2018[15]).

The process of data governance covered in the Data Governance Framework 1.0 is meticulous in setting forth basic principles for the implementation capacity, such that: i) data must be selected for regulatory outcomes; ii) compliance, security and privacy must be ensured; iii) standards and guidelines must be defined; and iv) human management and organisational culture must be involved. In this context, collaborative and cohesive data governance across the public sector is pivotal. The MDES and DGA are at the helm of fortifying good data management practices across the public sector towards greater integration. Yet, due to the decentralisation of power, responsibilities and information (covered in the previous sub-section "Leadership") and the lack of mature data governance standards, the public sector generally experiences low efficiency and effectiveness in implementation.

While data governance tools such as the Data Governance Framework 1.0 are sound conceptually, the government of Thailand still faces challenges in the implementation process at an operational level. Public sector organisations still struggle to implement good data management. For instance, the Department of Provincial Administration (DOPA) sits on the board of the DGA and is responsible for the citizen data registry and a data-sharing platform with the Ministry of Interior (MOI). The MOI, together with other line ministries managing data registers, still faces obstacles in data governance, standards, discoverability and quality for data sharing at an operational level with the public sector organisations it works directly with.

The signing of memoranda of understanding (MOUs) has been used for linking data among government agencies. As covered in Chapter 5, the DGA is piloting various projects such as the Government Data Exchange Centre (GDX), the Linkage Centre and the G-Cloud cloud computing tool. At the same time, the Steering Committee for Big Data, Data Centres and Cloud Computing is overseeing the formation of a centralised big data management system and a central cloud computing centre but still has not defined which government agency will be responsible for them due to the complexity and variety of datasets (Tortermvasana, 2018[15]). These nascent digital government initiatives may fail if co-ordination and the enforcement of centralised data standards are weak.

The DGA, as the leading public sector organisation responsible for ensuring that government agencies properly determine the purpose, control and verification of the management of their data, could provide greater assistance by providing more practical measures, guidelines and good practices on top of the Data Governance Framework. The DGA, the ONDE, the Digital Government Development Commission and the Steering Committee for Big Data, Data Centres and Cloud Computing could be the four government bodies through which co-ordination, implementation and compliance are secured for the proposed Action Plan for Public Sector Data across the public sector – with the latter two serving more of an advisory role.

In addition to the high ambitions and long-term goals set out in the broad 20-Year Digital Economy and Society Development Plan (2017-2036) or Digital Thailand, the government of Thailand needs to pay keen attention to developing the essential capacities for coherent implementation – particularly in involving and co-ordinating different policy areas and levels of government for coherent implementation. This area was identified to be a weakness in the governance of Thailand's open and connected government (OECD/ADB, 2019, p. 90[16]).

Apparently, the MDES intends to involve the academia in the Steering Committee for Big Data, Data Centres and Cloud Computing, since policies on data governance and metadata catalogues are led by both the minister and stakeholders from academia. Suan Dusit University (SDU) has collaborated in the creation of the Government Big Data and Data Analytics Centre to increase use cases. The DGA should also be involved in leading and co-ordinating this initiative since this task comes under its mandate of studying, researching, experimenting, endorsing and sponsoring academic works, research and innovation to enhance digital government development (see Key Objective 7 of Box 6.3).

Institutional data leadership and skills

Given the complex cross-cutting nature of the efforts and actions needed to build a data-driven public sector, the right management and organisational structures need to be put in place through institutional management frameworks that specify formal co-ordination processes and mechanisms for smooth and sustained project implementation among units in the ecosystem (Ubaldi, 2013, p. 34[17]). The results of the surveys conducted by the OECD for the purpose of this review show that government agencies in Thailand largely co-ordinate their own data management and initiatives – determining the roles, responsibilities, rights and duties for data operations from creation, storage, processing to use and dissemination. This results in a siloed approach that severely impedes the integration of databases and systems.

For instance, the Government Big Data Institute (GBDi) was established as a subsidiary of the MDES and DEPA to train public officials in big data skills. As presented in Chapter 4, this mandate is also undertaken by the DGA and OPDC (through the Thailand Digital Government Academy [TDGA]) and connects to Thailand's Skill Development Framework developed by the OCSC. The OCSC's framework would benefit from further clarifying its connections to the DGA Data Governance Framework, for instance by including data leadership and other related data competencies and skills as a subset of the digital roles described in the framework.

Still, for the level of data capacity to be translated into effective co-ordination and implementation, the government of Thailand would need to define a clear network of data leaders at the institutional level to promote better administrative co-ordination across the country, departments and provinces. Institutional networks are a growing priority for countries, as they enable stronger strategic co-ordination on the design and achievement of goals with a citizen-centric approach, more than just technical co-ordination (OECD, 2019, p. 40[1]). For instance, at the beginning of 2021, the UK announced the appointment of three senior Digital, Data and Technology (DDaT) leaders concurrently to strengthen the government's digital leadership strategically and enabler better co-ordination of the development and delivery of digital standards, controls, products and services leveraging data and emerging technologies. These three leadership appointments were the chair of a new Central Digital and Data Office (CDDO), the executive director of the CDDO and the new chief executive officer (CEO) of the Government Digital Service (GDS) – which have also received political backing from the prime minister (GOV.UK, 2021[18]).

The proposed Action Plan for Public Sector Data should have a proper institutional setup and co-ordination mechanism that identifies specific stakeholders for leadership and accountability. For instance, the Data Governance Framework 1.0 underscored that successful governance means that the person with the oversight role should have the responsibility for defining the scope, rules and policies around data (DGA, 2018, p. 10[9]). It also proposes a data governance structure for government agency personnel to carry out data supervision in their departments: i) a data governance council comprising the CEO, CDO, CIO and chief strategy officer (CSO); ii) a data steward team comprising the lead data steward and other data stewards covering the business, data and quality; and iii) wider data stakeholders comprising the data creators, users, managers and owners (DGA, 2018, pp. 52-56[7]) – which can be further enriched.

The DGA should support national, department and provincial government agencies to carry out the proposed data governance structures but in line with the agreed competency and skills frameworks for data to be decided by the OCSC. The DGA could oversee the specification of the roles, responsibilities and key performance indicators according to the operational context of different government agencies such as the missions and budgets, and in line with the Data Governance Framework.

Finally, a good strategy goes beyond setting up new government agencies, commissions and committees or designing new frameworks, plans and roadmaps. The details in the actual governance arrangements matter significantly to ensure successful sustainable execution. They should be lean, effective and clear to public officials. Most importantly, these governance arrangements should withstand changes in the political and administrative context and secure the sustainability of data leadership, capacity and capability in the long run, which is a common risk that several OECD member countries face.

Therefore, the government of Thailand could consider formalising more non-political and non-technical data leadership roles and embedding them under the leading public sector organisation on the Action Plan for Public Sector Data. Given Thailand's political context in recent years, the formal appointment of a top position in the DGA (i.e. National CDO or CIO) would be very helpful in reinforcing the leadership and capability of the DGA to design and implement data-driven policies and programmes across the public sector. As discussed in the previous sub-section "Leadership", this would constitute a critical asset for Thailand to materialising policy goals for a data-driven public sector in the long term.

Regulation

Regulation plays an important role in defining the set of rules around the use and treatment of data (OECD, 2019, p. 42[1]). As discussed in Chapter 3, the government of Thailand has risen to the act of solidifying and reinforcing the legislative support and guidance for its policies to build a data-driven public sector in recent years. In 2019, the National Legislative Assembly of Thailand (NLA) passed six technology-related legislations to improve and clarify the regulatory environment for public and private digital services:

- Electronic Transactions Act No. 3, B.E. 2562 (2019), and No. 4, B.E. 2562 (2019).
- Electronic Transactions Development Agency Act, B.E. 2562 (2019).
- Digital Economy and Society Council Act, B.E. 2562 (2019).
- Personal Data Protection Act, B.E. 2562 (2019).
- Cyber Security Act, B.E. 2562 (2019).
- Digitalisation of Public Administration and Services Delivery Act, B.E. 2562 (2019).

These efforts in digitalisation reform are notable. As discussed in Chapter 3, the Digitalisation of Public Administration and Services Delivery Act, B.E. 2562 (2019), was highlighted widely as the first digital government law in Thailand. It is intended to accelerate digital transformation in the public sector with a solid legal framework. Three focus areas are: i) digitalisation of processes and services using a citizen-centric approach; ii) data integration between government agencies to provide comprehensive digital services for citizens and businesses; iii) open government data in machine-readable formats to enable citizens and businesses to re-use and develop innovations – and the plans, rules and standards to elaborate on these legal provisions are still underway (Rohaidi, 2019[19]).

Yet, legislation is a first step but it does not guarantee effective and sustained implementation. During the OECD peer review mission in Bangkok, the Office of the Council of State under the PMO in charge of drafting the Digitalisation of Public Administration and Services Delivery Bill shared that the legislation is intended to change the public sector culture, enforce data sharing and facilitate the operations of the Government Data Exchange Centre (GDX) and Open Government Data Centre.

The prime minister of Thailand actively supports the Digitalisation of Public Administration and Services Delivery Act, B.E. 2562 (2019) but still faces resistance from various government agencies due to the lack of readiness and capability. As discussed in the previous chapters, both hard and soft regulatory instruments need to be enforced actively with strong co-ordinated efforts across the public sector. This process requires marked changes in the organisational structure and culture including human resources, digital infrastructure and public trust. This proves the point that legislation and regulation need to be accompanied by agile, innovative institutional approaches that enable strategic and anticipatory change according to the circumstances.

As discussed in Chapter 3, regulations may slow or hinder the process of data integration. There needs to be a balance between flexibility and scalability on one end, and preserving the complexity of control and compliance for data integration on the other that prevents fragmentation (OECD, 2019, p. 33[1]).

Regulations around data governance should allow for purposeful and organic changes in the environment and among actors. Such a balance also provides experimental freedom for new initiatives that are focused on solving problems for better public outcomes and free from policy delivery constraints (OECD, 2019, p. 78[1]).

One area of regulatory tension has been identified to be between data protection and data sharing. The ONDE, responsible for designing digital economy and society policies, highlighted that it has not embarked on open data or data-sharing initiatives due to legislative restrictions and the administrative burden emerging from the Personal Data Protection Act. The balance between a flexible and structured approach can help to foster common understanding, alignment and coherence of data initiatives. It creates greater support for concerted actions when addressing challenges and delivering results (OECD, 2019, p. 33[1]).

The government of Thailand could, for instance, elaborate on soft legal and regulatory instruments such as codes of practice, recommendations, standards and guidelines that specify data integration and sharing, aimed at fostering these cultural changes, developing the understanding and skills to unlock the potential of accessing, sharing and using data ethically.

Leveraging data access and sharing to deliver public value

This second section looks at what the government of Thailand needs to improve the technical delivery layer of data architecture, data infrastructure and data value cycle to increase the availability, accessibility and use of data in data sharing and open data practices in the public sector.

While a strong focus on technical issues concerning data governance can be misleading and weaken the approach towards the adoption of relevant policy decisions on data (OECD, 2019, p. 27[1]), underpinning the transition to a data-driven public sector calls for the definition of a complex set of data access, collection and sharing arrangements across sectors, including standards and guidelines, to support the delivery of public value.

A key working principle of the DGA's G2G, G2C and G2B infrastructure, platforms and enablers is to link and exchange data and unlock greater public value. As explored in Chapter 5, the DGA aims to create "an effective data management system [that is] accurate, complete, updated and connectable promptly and securely" (DGA, 2018, p. 12[9]) to be used for developing new platforms, tools and services such as the Government Information Network (GIN) for connecting government agencies at all levels to facilitate a wide range of applications, the Government Data Exchange Centre (GDX) for digitally transferring documents among agencies and the One-Stop Service for citizens to access public services.

Most initiatives for data integration are oriented around identifiable data on citizens and businesses and data related to national security and critical infrastructures, following the first phase of integrating government databases directed by the Prime Minister Operations Centre (PMOC) and the Steering Committee for the Integration of Government Databases (EGA/MICT, 2016[20]). While the central government is prioritising data, information and systems integration as the foundation for a data-driven public sector at a strategic level (EGA/MICT, 2016[20]), there is a considerable lack of operational expertise and understanding to deal with the heterogeneity of the data and the complexity of data integration at the executional level. This is reflected in a missing Action Plan for Public Sector Data for implementation as described in the previous section.

As identified in the previous sub-sections, a key challenge faced by the government of Thailand is the execution of the data plans and especially at the departmental and provincial levels. There needs to be a stronger understanding of what data are available or not, and if those data are valuable, compatible and interoperable to be used and re-used, this together with the experiences and capabilities related to data management and analytics that need to be consolidated – such that data governance can be carried out effectively. These were the challenges for the use of national data registries that were often cited in the surveys conducted by the OECD for the purpose of this review.

There are different types of data with widely different data value cycles and economic and social value. It would be advisable for the government of Thailand to have a comprehensive and coherent approach towards organising, categorising and integrating government data. Doing this step correctly can provide the leverage to achieve developments in data sharing and reinforce public trust in the government's use of data – together with open government data as explored in Chapter 7. In this light, this section will reveal the overlooked areas and explore opportunities to establish a solid data architecture (design) and infrastructure (technical) that will reap the double-sided benefits of data sharing and strengthening the accountability and trust among stakeholders in the ecosystem.

Data integration: Infrastructures, standards and guidelines

The government of Thailand has set policy milestones for establishing several one-stop services such as PromptPay, Biz Portal, Farmer ONE, the Linkage Centre, e-Social Welfare, GIN, the Government Application Centre (apps.go.th), the Open Government Data Centre (data.go.th) and the Government Data Exchange Centre (GDX) (Thiratitayangkul, 2019[21]). This has culminated into the launch of a mobile application CITIZENinfo in late 2019, a one-stop service that has a citizen and a business portal, offering information on public services from government agencies nationwide. It functions like a government kiosk and an integrated e-services platform that uses digital documentation like the digital ID and runs on integrated big data and analytics (Thiratitayangkul, 2019[21]). However, the OECD found that these one-stop services are driven more by an e-government approach and a one-way provision that is not fully digital, as discussed in Chapter 5. The leap to being truly data-driven will require stronger efforts to build and strengthen a holistic, coherent, scalable and agile data architecture and infrastructure.

Government data are not naturally harmonised because government agencies with different responsibilities from various policy areas have different datasets and formats (Ubaldi, 2013, p. 31[17]). Several public sector organisations express their aspiration and plans in the use of big data and data analytics. Nevertheless, the main barrier that constantly resurfaced through the interviews conducted and the data collected within the framework of this review is the lack of standards and guidelines, in addition to flawed human resource capability, which made the process of data management and analysis challenging. The government of Thailand currently has policies, standards and guidelines on data security and stability, data disclosure, data link and exchange, data confidentiality, open data, personally identifiable information, data innovation design and data governance assessment (DGA, 2018, p. 45[9]). However, focusing also on the data generation stage would help to secure integration in the later stages of the data value cycle. So far, the guidelines and standards available address data access and sharing once the data has been already generated or assume data assets are discoverable and accessible.

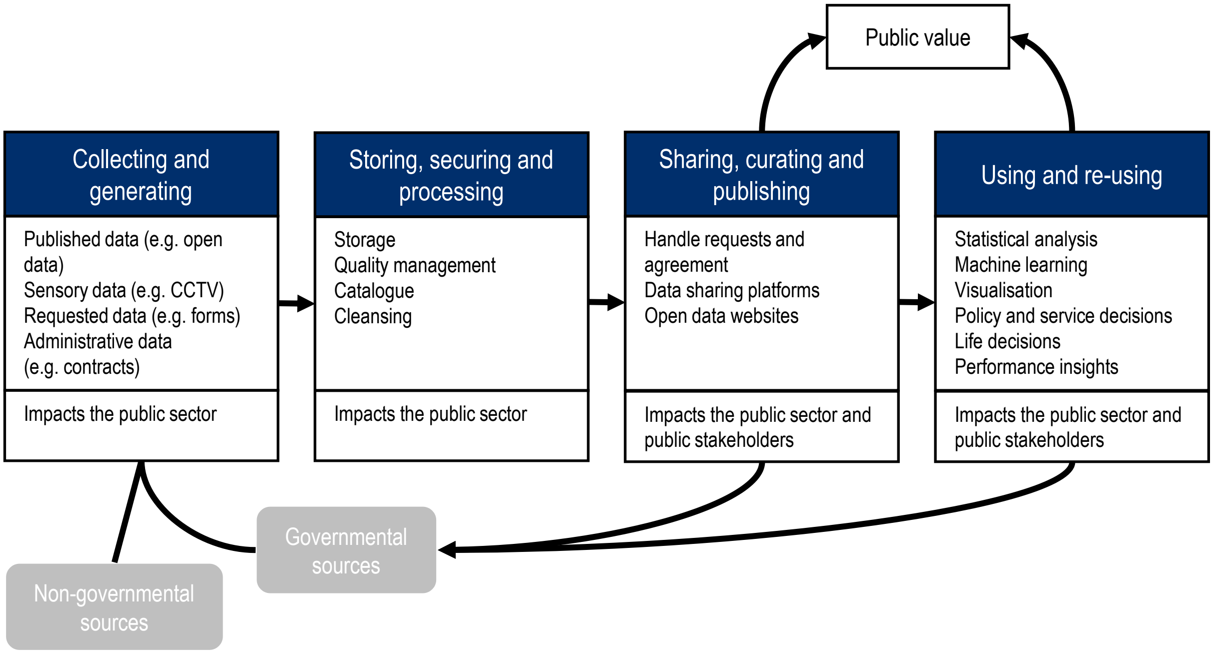
A good example is the National Information Committee, which was under the Ministry of Information and Communication Technology (MICT) and now the MDES. The National Information Committee drives information policy, manages the geographical information system (GIS) and geospatial datasets from 30 public sector organisations. Still, it faces difficulty in data discoverability and data ownership for a large number of datasets under its purview. In response to such a challenge, different countries have had different responses. Korea and the UK have developed a single data inventory for the government to provide ease of internal data discoverability and data re-use. Korea has especially taken practical steps to put the needs and structure of base data registries into legal records to simplify the sourcing and curation of datasets (OECD, 2019, p. 64[1]). Most relevant is Italy, which developed technical regulations on the territorial data of public administrations and a national metadata catalogue to guarantee the discoverability and clarity of spatial data and related public services (OECD, 2019, p. 44[1]).

Another example is the Ministry of Commerce (MoC) that expresses strong support for digital integration and greater alignment and co-ordination in the development of digital policies and initiatives. It has a pilot project to share web service data with the Ministry of Agriculture and Cooperatives (MOAC) and the Rice Department, in view of real-time data-sharing projects for maize, palm oil and sugar in the future. However, as shared during the OECD peer review mission in Bangkok and the OECD survey, the MoC has not yet been able to complete the basics such as mapping the business ecosystem and datasets or harmonising operating models and metadata standards. This reinforces the message that the government of Thailand needs stronger data policies, standards and guidelines with compliance for the implementation of its high ambitions for a data-driven public sector to come to fruition.

Data value cycle: Gaps, challenges and solutions

The data value cycle presents the crossroads and synergies of the most strategic, tactical aspects of data governance (e.g. policies and regulations) with the technical aspects (e.g. architecture and infrastructure for data management, open data and sharing). It is a continuum of inter-related stages where different stakeholders add value and contribute to data re-use (OECD, 2019, pp. 46-47[1]). Looking at the data value cycle, the government of Thailand is still held back in the first two phases of collection, generation, storing, securing and processing (Figure 6.8).

Figure 6.8. The data value cycle


Public value
Collecting and generating
Published data (e.g. open data)
Sensory data (e.g. CCTV)
Requested data (e.g. forms)
Administrative data (e.g. contracts)
Impacts the public sector
Storing, securing and processing
Storage
Quality management
Catalogue
Cleansing
Impacts the public sector
Sharing, curating and publishing
Handle requests and agreement
Data sharing platforms
Open data websites
Impacts the public sector and public stakeholders
Using and re-using
Statistical analysis
Machine learning
Visualisation
Policy and service decisions
Life decisions
Performance insights
Impacts the public sector and public stakeholders
Governmental sources
Non-governmental sources

Source: van Ooijen, C., B. Ubaldi and B. Welby (2019[4]), "A data-driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance", https://dx.doi.org/10.1787/09ab162c-en.

This explains why several public sector organisations in Thailand are still struggling with the heterogeneity of government data and the complexity of data integration. They are unable to progress to the third and fourth stages of creating value from data and data-driven processes. Oftentimes, governments get stuck in the first two stages of understanding what kind of government data exists, what form and how they can be used – in order to organise, categorise and integrate the data after. They also need to address issues regarding the interoperability of systems and standards and quality of data. The role of leading bodies such as the DGA, the Digital Government Development Commission, the MDES and committees such as the Steering Committee for Big Data, Data Centres and Cloud Computing will remain key for this purpose.

The DGA is charged with the mandate and task of increasing internal connectivity and integration for interoperability via secured networks or platforms. In addition to the aforementioned GIN and Government Data Exchange Centre (GDX), several more open data and data-sharing projects include: the Digital Government Platform to link important public sector data among more than 620 government agencies through the Single Sign-On system, the e-CMS Version 2.0 on G-Cloud and the government application programming interface (API) system; the government information infrastructure that hosts more than 2 895 open datasets on the Open Government Data Centre (data.go.th); the Government Information Centre (info.go.th) for citizens to access government services datasets and comprehensive service manuals (DGA, 2018, pp. 33-39[9]).

To strengthen the efficacy and efficiency of the Data as a Service (DaaS) approach presented in Chapter 5, reinforcing the role of the DGA as the leading public sector organisation to set, co-ordinate, align and enforce the data policies and standards in the early stages of the data value cycle (e.g. data generation) would serve well to propel data integration and re-usability towards value creation across the public sector. It would also be helpful to attribute greater accountability to the DGA for this process, as leadership and accountability are mutually reinforcing. More formal requirements through legal and regulatory frameworks are needed to secure responsibility, integrity and consistency in contributing government data to the data-sharing platforms developed by the DGA, including the open government data portal. Emphasising data stewardship and ownership by the hundreds of government agencies or private sector organisations that are involved is also important for consistency and compliance.

While the government of Thailand is progressing well by creating new digital tools, platforms and services that accelerate data integration, open data and data sharing, dedicating more resources to replicate and scale standardised data architectures and infrastructures across the digital economy and society will unlock smoother and more trustworthy access and sharing of data within and outside the public sector. Having in mind Thailand's regulatory momentum on digitalisation, designing data policies, standards and guidelines in legislation and executive decrees that unlock better harmonisation and co-ordination at all levels of the government would be a boon in strengthening a data-driven public sector. Priorities to be addressed include data accessibility, data ownership, data sharing, data use, data interoperability, metadata, data skills for public officials and engagement with the wider ecosystem of the public sector, private sector and civil society stakeholders.

Establishing the role of data for public trust

The previous sections explored the role and importance of data governance in leveraging data access and sharing and establishing a data-driven public sector. These are crucial foundations and layers for the government of Thailand's digital transition. Yet, in order for the country to truly reap sustainable benefits in economic and social development, the government of Thailand also needs to prioritise the creation of a trustworthy environment to promote integrity and accountability in the use of data for policy making and the delivery of public services. This is even more critical in times of crisis, such as the COVID-19 pandemic, where governments are faced with the intense burden to ensure a functioning state, the continuous delivery of public services and a resilient and equitable economic recovery. With social distancing becoming the new norm, the digital space is taking up a bigger share in the economy and society.

The trustworthy use of data to understand citizens and businesses' needs, adjust and improve processes with the intent to meet these needs, is fundamental. Furthermore, the role of data governance in securing and reinforcing public trust in times of crisis has become an increasingly important case since incidents of data misuse and abuse by governments and businesses in different parts of the world have emerged and catalysed regulations on data protection and their ethical, transparent and secure data use.

Public trust in the management and treatment of data is a crucial precondition for maximising the gains of digital transformation through effective and efficient policy implementation. A trustworthy government that is open and connected requires a solid data framework for government processes and public services that can be carried out with the highest level of confidence. According to the OECD report *Trust and Public Policy* (Table 6.2), five determinants of institutional trust are responsiveness, reliability, integrity, openness and fairness. Increasing these outcomes can help governments to restore, maintain and increase the level of trust in them (OECD, 2019, p. 104[1]). Furthermore, an OECD working paper highlighted that citizens' well-being can be improved when digital governments use data to become more responsive, protective and trustworthy – which covers aspects of ethics, privacy, transparency and security (Welby, 2019, p. 43[22]) (Box 6.6).

Table 6.2. Determinants of citizens' trust in public institutions: Competencies and values

Trust component	Government mandate	Key elements	Objective
Competency – Governments' ability to deliver to citizens the public services they need at the level of quality they expect	Provide public services	• Access to public services regardless of the social and economic situation • Quality and timeliness of public services • Respect in public service provision, including response to citizen feedback	Responsiveness
	Anticipate change, protect citizens	• Anticipation and adequate assessment of evolving citizen needs and challenges • Consistent and predictable behaviour • Effective management of social, economic and political uncertainty	Reliability
Values – Drivers and principles that inform and guide government action	Exercise power and use public resources ethically	• High standards of behaviour • Commitment against corruption • Accountability	Integrity
	Inform, consult and listen to citizens	• Ability to know and understand what government is up to • Engagement opportunities that lead to tangible results	Openness
	Improve socio-economic conditions inclusively	• Pursuit of socio-economic progress for society at large • Consistent treatment of citizens and businesses over the fear of capture	Fairness

Source: OECD (2017[23]), *Trust and Public Policy: How Better Governance Can Help Rebuild Public Trust*, https://doi.org/10.1787/9789264268920-en.

Box 6.6. Policy recommendations for improving citizens' well-being

Governments that commit to a digital government agenda can improve the well-being of their citizens by using digital technology and data to be responsive, protective and trustworthy.

Responsive governments:

- Involve citizens throughout the design and delivery lifecycle to understand their needs.
- Proactively reach out to citizens and involve them in the design and delivery of services.
- Design the end-to-end experience of services, not just the implementation of technology.

Protective governments:

- Prioritise the protection of the public from external digital security threats.

- Ensure that provided services are reliable and secure.
- Rethink regulation to focus on outcomes rather than specific technologies.

Trustworthy governments:

- Find a balance between online safety and democratic freedoms to build public trust and confidence.
- Deliver high-quality, reliable services that understand citizens and are open to feedback.
- Show citizens what the government is doing and empower citizens to manage their data.

Source: Adapted from Welby, B. (2019[22]), "The impact of digital government on citizen well-being", https://dx.doi.org/10.1787/24bac82f-en.

The government of Thailand understands the importance of governing and managing data with trust as the backbone to improve citizens' well-being. The DGA's goal of digital government is "upgrading the work process and public services with appropriate digital technologies [while] taking benefits, needs and convenience of the people as key priorities" and this "also includes the disclosure of government data in digital form for transparency, public participation promotion, innovation development on all levels" (DGA, 2018, p. 12[9]). Its digital government services have qualified for international standards, such as the Cloud Security Alliance (CSA) Security, Trust and Assurance Registry that enhances transparency in cloud computing services and the Business Continuity Management Systems (BCMS) that enable holistic management of threats to business operations (DGA, 2018, p. 30[9]).

Trust is also a major component of the 20-Year Digital Economy and Society Development Plan (2017-2036) or Digital Thailand. The sixth strategy in this plan is focused on building trust and confidence in the use of digital technologies by updating laws and regulations, encouraging investments and ensuring security (Segkhoonthod, 2017[24]). This also ties tightly into the 6th strategy of the 12th National Economic and Social Development Plan (2017-2021) that aims to root out corruption and achieve good governance in the public administration (Segkhoonthod, 2017[24]). Measures taken under this strategy towards data ethics and the use of digital technology and tools are most critical in determining public outcomes.

Enabling a trustworthy environment for data access, sharing and re-use of data through formal legislation and self-regulation are two key reinforcing mechanisms to securing public trust – keeping in mind the determinants of trust in public institutions are responsiveness, reliability, integrity, openness and fairness, and are maintained through regulations and practices in the use of data (OECD, 2019, p. 102[1]). In the following four sub-sections on ethics, privacy, transparency and security, country examples and policy recommendations on using data for public trust will be elaborated in the context of Thailand.

Ethics

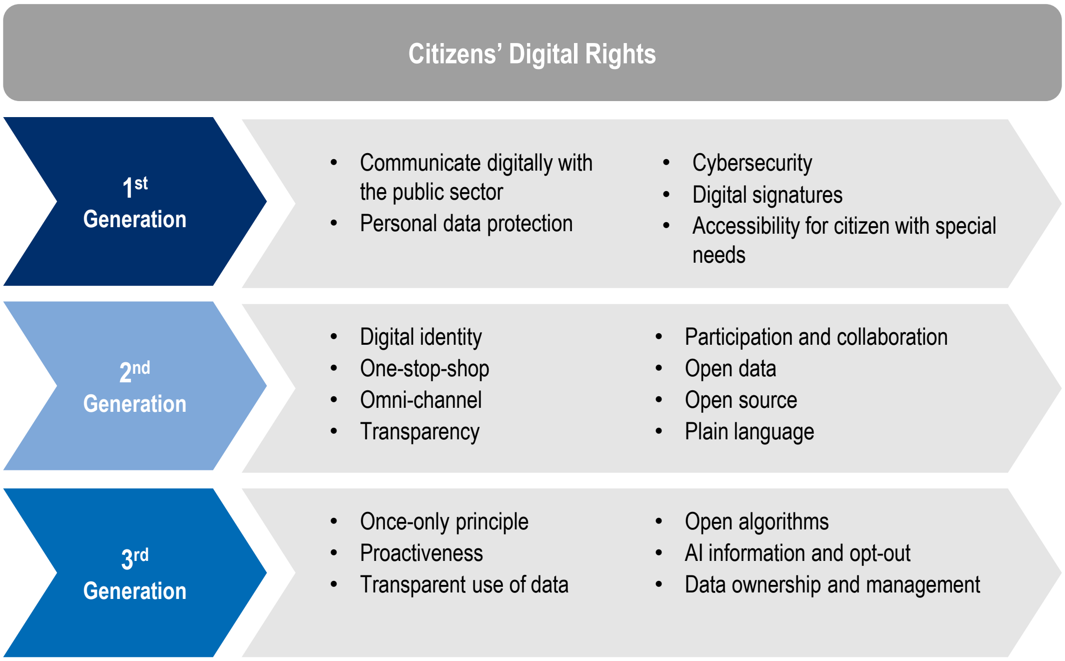
As discussed in the OECD report *The Path to Becoming a Data-Driven Public Sector*, data ethics is a branch of ethics that "studies and evaluates moral problems related to data (including generation, recording, curation, processing, dissemination, sharing and use), algorithms (including AI, artificial agents, machine learning and robots) and corresponding practices (including responsible innovation, programming, hacking and professional codes), in order to formulate and support morally good solutions (such as right conduct or right values)" (Floridi and Taddeo, 2016[25]; OECD, 2019, p. 109[1]).

Globally, citizens' attitudes towards data practices in the public and private sectors are changing quickly and the interest in ethical approaches to data management is growing due to the advancement of digital technology and collection of a massive amount of data, leading to its extensive use and the emergence of cases of data misuse and abuse. These circumstances call for public leadership that can establish and ensure a culture of ethical and responsible use of data. Handling data ethically can balance innovation with data protection while placing data subjects and users at the centre of the public service design process.

This circles back to the importance of involving the public, private sector and civil society stakeholders to engage in the process to build trust (OECD, 2016, pp. 157-158[26]). Public communication and participation with these stakeholders to agree and align on a set of behaviours and practices around data ethics can encourage transparency and ownership to abide by the ethical management of data.

A discussion of data ethics should also involve a discussion of digital rights. Inspired by the evolution of human rights and fundamental freedoms in relation to the digital age, the OECD designed a tentative framework that classifies digital rights roughly into the first, second and third generations (Figure 6.9) (OECD, 2019, p. 107[1]).

Figure 6.9. Digital rights towards a citizen-driven digital transformation



Citizens' Digital Rights

1st Generation

- Communicate digitally with the public sector
- Personal data protection
- Cybersecurity
- Digital signatures
- Accessibility for citizen with special needs

2nd Generation

- Digital identity
- One-stop-shop
- Omni-channel
- Transparency
- Participation and collaboration
- Open data
- Open source
- Plain language

3rd Generation

- Once-only principle
- Proactiveness
- Transparent use of data
- Open algorithms
- AI information and opt-out
- Data ownership and management

Source: OECD (2019[1]), *The Path to Becoming a Data-Driven Public Sector*, https://doi.org/10.1787/059814a7-en.

The first generation of digital rights falls under the civil and political category and should be regarded as fundamental: the right to communicate digitally with the public sector, the right to personal data protection and the right to cyber security to name but a few. The second generation of digital rights falls under the socio-economic category and emerged from the rapid advancement of digital technologies in platforms and portals: the right to a digital identity, the right to access one-stop-shops and open data to name but a few. The third generation of digital rights falls under the collective developmental category that has become important due to the emergence of new technologies like AI: the right to the transparent use of data, the right to access open algorithms and the right to data ownership and management to name but a few.

Most OECD member countries have legislative provisions that cover up to the second generation of digital rights. Finding ways to protect these digital rights is crucial but not enough to create a safe operational environment of trust that not only complies with regulatory provisions but also adheres to values such as fairness, transparency, agency in the use of data at the more operational level. Therefore, a formal legalistic approach through "hard" regulations is best paired with "soft" frameworks and guidelines that are embedded deeply in the working culture and encourage self-regulation spontaneously.

Ethical approaches play a pivotal and significant role to guide the behaviours of public administrators and public officials in the public sector. They ensure that data will be managed in ways that do not harm or undermine the utility of others, even when done in a lawful way. For instance, collecting data from COVID-19 patients such as their age, occupation, affiliations and addresses may help with contact tracing but this could be unethical if their personal safety is compromised. Governments, therefore, play a fundamental role in determining ethical practices in government processes that manage data and should aim at guiding decision making and informing on ethical behaviour around data (OECD, 2019, p. 109[1]).

The government of Thailand has begun building the legal foundations in recent years to explore, define and guarantee the first and second generations of digital rights with some incorporation of the third generation. However, it has not yet designed ethical principles, frameworks or guidelines on data management and use in the public and private sectors. This presents an opportunity to consider various paths to achieving the goal of shaping behaviour that is conducive to a healthy data-driven public sector that centres on the human aspects of data management and respects the rights of citizens.

These data ethical frameworks and guidelines should contain principles, information and approaches to conduct value-driven practices and decision making that aim to increase understanding of what it means to manage and use data in a way that places fundamental rights and freedoms at the core of government practice and how this translates to specific actions.

In light of the above, the OECD launched the *Good Practice Principles for Data Ethics in the Public Sector* in 2021 as a means to provide a common values-based ground for the trustworthy management of data by public entities (Box 6.7).

Box 6.7. The Good Practice Principles for Data Ethics in the Public Sector

The Good Practice Principles for Data Ethics in the Public Sector support the ethical use of data in digital government projects, products and services to ensure they are worthy of citizens' trust. The Good Practice Principles provide a set of specific actions which can support their implementation.

1. Manage data with integrity.
2. Be aware of and observe relevant government-wide arrangements for trustworthy data access, sharing and use.
3. Incorporate data ethical considerations into governmental, organisational and public sector decision-making processes.
4. Monitor and retain control over data inputs, in particular those used to inform the development and training of AI systems, and adopt a risk-based approach to the automation of decisions.
5. Be specific about the purpose of data use, especially in the case of personal data.
6. Define boundaries for data access, sharing and use.
7. Be clear, inclusive and open.
8. Publish open data and source code.
9. Broaden individuals' and collectives' control over their data.
10. Be accountable and proactive in managing risks.

Governments that commit to a digital government agenda can improve the well-being of their citizens by using digital technology and data to be responsive, protective and trustworthy.

Source: OECD (2021[27]), *Good Practice Principles for Data Ethics in the Public Sector*, https://www.oecd.org/gov/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.htm.

At the national level, the UK Data Ethics Framework specifically sets out principles on the appropriate use of data in the public sector and continues to be iterated through detailed guidance, a workbook to be used for new data projects and workstreams (GOV.UK, 2018[28]).

In a later stage, enforcement and compliance with ethical practices can be executed via an independent government agency, with a lead role in supporting other public sector organisations in capacity building and data management. The DGA has a strong fit for this role with its anti-corruption policy and mandate in "supporting and promoting personnel at all levels to be aware of the importance of behaving in compliance with morals, ethics and anti-corruption awareness" (DGA, 2018, p. 83[9]). For this to be achieved effectively, the DGA could be given the power and authority across the public sector and country in supervising and monitoring the practices in accordance with the laws and regulations around data management and use. While the Personal Data Protection Committee (PDPC) is the supervising authority for data protection, the DGA could be the main steward for the government's trustworthy data management and use. Both bodies will need to co-ordinate strategically and closely, set strategies and exchange information. They should test ideas, design principles and measure risks continually as data are used and new technologies such as AI are applied on top of them.

To strengthen the DGA's efforts in data ethics, it could create a data ethics advisory group like New Zealand. New Zealand's Data Ethics Advisory Group is headed by the Government Chief Data Steward (GCDS) (i.e. a position non-existent in Thailand by law) and the group's purpose is to assist the government to understand, advise and comment on issues around new and emerging uses of data. Seven independent experts from different fields like privacy, human rights law and innovation, which are relevant to data use and ethics, were appointed as members. Diversity of perspectives is ensured too, with one position reserved for a member of the Te Ao Māori Co-Design Group to support Māori data governance (Stats NZ, 2019[29]).

Such a data ethics advisory group can support the DGA by looking into new initiatives in the early stage of development, such as exploring the idea of using data trusts to facilitate ethical and trustworthy data sharing. Similarly, in this area, ensuring the success of establishing an ethical environment will require consistent communication and engagement over these ethical frameworks, guidelines and principles in the data access and sharing ecosystem that include actors from the private sector and civil society.

Privacy

Privacy refers to the protection of rights of data subjects and a central part of this is consent to the collection, processing and use of data from these data subjects. This is a huge area of concern for data subjects, especially on the treatment of sensitive and personally identifiable data. A reasonable and balanced approach to data protection can secure the value of data sharing, such as the delivery of cross-border public services (OECD, 2019, p. 25[1]).

As such, it is important to address the following issues when it comes to publishing and using data in an open data and data-sharing ecosystem: which public sector organisations hold the data, have the right to access the data, have made an enquiry about the data, use the data and for what purposes; the right to provide data once only to the government; and the right to agree or refuse permission for data provided to be shared and re-used by other public sector organisations (OECD, 2019, p. 113[1]).

Many governments have begun to create formal legislation and accompanying frameworks and guidelines to protect data subjects' privacy for both citizens and businesses across the data value cycle. The European Union General Data Protection Regulation (GDPR) was landmark legislation that created a global upwards convergence towards high standards of data regulation protection after its implementation in 2018. In the implementation of the GDPR, the UK ensured that the provisions of the Data Protection Act 2018 are in line with the privacy safeguards and code of practice for data sharing in the Digital Economy

Act 2017 (Chapter 5: “Sharing for research purposes”) to ensure that data will not be misused or shared indiscriminately (GOV.UK, 2020[30]).

In the effort to design and offer more citizen-centric services, the government of Thailand has committed to balancing the security of lives, assets and public data with the need to address constant changes of public needs and facilitating public service delivery. To protect privacy and allow users to give consent with explicit knowledge of how the data is collected, processed and used, the government of Thailand passed the Personal Data Protection Act, B.E. 2562, in May 2019 and that came into full force in May 2020.

The Personal Data Protection Act, B.E. 2562 (2019), established the PDPC, with the vice-chairperson as the Permanent Secretary of the MDES and the directors as the Permanent Secretary of the PMO, the Secretary-General of the Consumer Protection Board, the Director-General of the Rights and Liberties Protection Department and the Attorney General (ETDA, 2019[31]). This follows from the Official Information Act, B.E. 2540 (1997), that had specific provisions to prevent the misuse of personal data by public officials and the right for citizens to know how their data are being used by public sector organisations.

The Digitalisation of Public Administration and Services Delivery Act, B.E. 2562 (2019), also stipulates under Section 14 that government agencies receiving data from another public sector organisation for the purpose of improving public administration and services should keep the data securely and that there should be no disclosure or transfer of such data to persons without the right to access it.

The Electronic Transactions Development Agency (ETDA) said during the OECD peer review mission to Bangkok that while promoting the National Digital ID (NDID) project, it also plans to raise awareness in the public sector and among citizens and businesses on privacy and how to protect their data in using digital tools. It was involved in the drafting of the Personal Data Protection Act. In May 2018, the MDES set up a Data Protection Knowledge Centre (DPKC) as the centralised unit to create awareness of data protection in the public and private sectors, with the ETDA as the operator and lead. In this respect, it would be ideal for the ETDA to continue in its leadership on securing privacy for data subjects in the treatment of public sector data, focus on education and building an awareness and working culture of practising data protection to build a safe environment until the office of the national PDPC is fully operational.

It could also consider fostering interoperability with other privacy frameworks to enable cross-border data flows, such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 2013[32]) and Regulation (EU) 2016/679 GDPR (van Ooijen, Ubaldi and Welby, 2019[4]).

Transparency

Transparency is about creating an open and trustworthy environment where policy and government information, decisions, processes, frameworks and rationales are made known to the public in a timely, accessible and comprehensible manner, which has an effect of increasing public officials’ accountability to each other and the public (OECD, 2019, p. 115[1]). This approach has direct applications on how personal or sensitive data is used by public sector actors, by whom, for what purpose and with what outcomes. With emerging technologies, transparency about how data is used and processed is fundamental for public trust and the good use and scaling of machine learning.

As the DGA of Thailand continues to create data policies, standards and guidelines on open data, data sharing and the re-use of data in the public sector, it could consider opening its actions, sharing data informing decisions processes and performance to public scrutiny as a way of gaining public trust. This often serves as a powerful and practical tool to gain the support and trust of citizens and businesses in the complex process of digitalising the government and public sector, since it allows them to see, understand, know how various data subjects’ data are used and therefore participate in the best possible way to create value for the economy and society.

Citizens can have the chance to contest should the data seem biased or wrong, which can help to augment the quality of data, fairness and value creation. Finally, the policies, standards and guidelines centred on openness also serve as one of the key pillars for when the government starts to incorporate more AI, to make the data processing sustainable and trustworthy – as agreed on by 20 countries of the OECD Thematic Group on Emerging Technologies (Ubaldi et al., 2019, p. 21[33]).

In Thailand, transparency in a data-driven public sector can be increased with the exposure of the data and algorithms. This is in line with a provision in the GDPR on the right to be informed about the existence of automated decision making. Principle 6 of the UK Data Ethics Framework also specifies that all activity in data science should be done "as open and accountable as possible" (GOV.UK, 2018[28]). France's Digital Republic Law no. 2016-1321 of 7 October 2016 aims to build a trustworthy and transparent digital and data-driven public sector through a legal framework that protects people's personal data and guarantees transparency of local and municipal government data (Dreyfus, 2019[34]).

Security

Security involves the management of risks around the treatment of public sector data by the government, to prevent any unauthorised access and use (OECD, 2019, p. 116[1]). To strengthen the foundation of public trust in how the public sector manages and uses data, citizens and businesses should know that the government is protecting the data from potential risks. Furthermore, cyberattacks can be costly for the country in terms of financial, economic, social, geopolitical and national security – damaging or impairing government processes and public services.

In line with plans for building Digital Thailand, the government of Thailand is ramping up efforts to secure the digital architecture and infrastructure in the public sector by consolidating the legislation, regulations and institutions. It plans to improve Thailand's ranking in the International Telecommunication Union (ITU) Global Cybersecurity Index with the development of national security policy, critical information infrastructure and standard operating procedures (Boonnoon, 2018[35]).

Thailand's Computer Crime Act, B.E. 2550 (2007), provided a definition of computer-related crimes and authorised government officials to investigate them. Amendments in the Computer Crime Act No. 2, B.E. 2560 (2017), further clarified the ambiguity of illegal content and defamation and improved the efficiency and integrity of the law enforcement process. It also aimed to prevent hacking data and information that could be wrongfully exploited. But in the past years, the government has done a minimal amount operationally to respond to the thousands of cyberthreat incidents and government agencies still have a poor capacity to respond to cyberthreats (Leesa-Nguansuk, 2019[36]). The Cyber Security Act, B.E. 2562 (2019), aims to change this with the creation of a National Cyber Security Committee, the National Cyber Security Agency (NCSA) and new rules to handle cyber threats.

The NCSA is chaired by the deputy prime minister and joined by the Minister of Digital Economy and Society, and has appointed seven cyber security expert commissioners. The NCSA will serve as Thailand's key communication centre and data hub for cyber security, to fight illegal data piracy and cyber security breaches in its digital infrastructure. It will be receiving a budget of BHT 500 million to BHT 1 billion for this purpose, co-operating with Cisco Thailand to train 1 000 security personnel and oversee the Thailand Computer Emergency Response Team (ThaiCERT) that used to be under the jurisdiction of the ETDA (Boonnoon, 2018[35]). The ETDA will then play a supporting role, continuing to provide licenses for digital identities and signatures and define security standards for data exchange (Boonnoon, 2018[35]).

Since Thailand has just begun its efforts in security, focusing on the development of an independent national digital security strategy with detailed policies, directions and guidelines for public sector organisations would be a strategic next step. Many OECD member countries have also identified digital security as a high priority and developed standalone strategies (OECD, 2019, p. 116[1]). Korea's strategy imparts authority to the National Information Resources Services for centralised co-ordination and focuses on best practices. The UK has a specific chapter on digital security in its national digital strategy and another separate National Cyber Security Strategy (2016-2021). Its National Cyber Security Centre is charged with building cyber security partnerships across the public and private sectors, providing cyber incident response and liaising with the national security services.

Lastly, digital security skills are a cornerstone – extensive training in cyber security capability should ensure that the country has a sustainable supply of home-grown cyber professionals that can meet the demands for a digital economy and society. Thailand will need to do the same and proceed in the execution phase with strong governance and co-ordination.

References

Boonnoon, J. (2018), “4 draft digital laws ready for Cabinet as govt boosts cybersecurity”, https://www.nationthailand.com/Startup_and_IT/30353553 (accessed on 4 May 2020). [35]

DGA (2018), *Annual Report 2018*, Digital Government Development Agency, Bangkok, https://www.dga.or.th/upload/editor-pic/files/AR_ENG_DGA-2018.pdf (accessed on 22 April 2020). [9]

DGA (2018), *Data Governance Framework Version 1.0*, Digital Government Development Agency, Committee on Digital Governance and Disclosure Process Studies, Bangkok, https://tdga.dga.or.th/index.php/th/send/9-document/388-data-governance-framework (accessed on 9 April 2020). [7]

Die Bundesregierung (2020), *Gemeinsam Datenpolitik gestalten: Öffentliche Konsultation zur Datenstrategie, Digitalisierung*, https://www.bundesregierung.de/breg-de/themen/digitalisierung/konsultation-datenstrategie-1761664 (accessed on 14 January 2021). [14]

Dreyfus (2019), *France: Public Service and Processing of Personal Data*, Dreyfus, https://dreyfus.fr/en/2019/08/05/public-service-and-processing-of-personal-data. [34]

EGA/MICT (2016), “Thailand’s 3 year Digital Government Development plan”, Electronic Government Agency/Ministry of Information and Communication Technology, Bangkok, https://www.transparency.org/whatwedo/publication/peoples_ex. [20]

ETDA (2019), “Personal Data Protection Act, B.E. 2562 (2019)”*, Government Gazette*, No. 136, Electronic Transactions Development Agency, Bangkok, https://www.etda.or.th/app/webroot/content_files/13/files/The%20Personal%20Data%20Protection%20Act.pdf. [31]

Floridi, L. and M. Taddeo (2016), “What is data ethics?”, *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, Vol. 374, http://dx.doi.org/10.1098/rsta.2016.0360. [25]

GOV.UK (2021), “Government strengthens digital leadership”, https://www.gov.uk/government/news/government-strengthens-digital-leadership (accessed on 15 January 2021). [18]

GOV.UK (2020), *Guidance: Digital Economy Act 2017 Part 5: Codes of Practice*, Department for Digital, Culture, Media & Sport, Cabinet Office, Home Office and UK Statistics Authority, https://www.gov.uk/government/publications/digital-economy-act-2017-part-5-codes-of-practice [30] (accessed on 18 January 2021).

GOV.UK (2018), *Guidance: Data Ethics Framework*, Department for Digital, Culture, Media & Sport, https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework (accessed on 3 May 2020). [28]

Ladley, J. (2012), *Data Governance: How to Design, Deploy and Sustain an Effective Data Governance Program*, Morgan Kaufmann Publishers. [6]

Leesa-Nguansuk, S. (2019), "ThaiCert moving to NCSA under new law: Cyber-infrastructure protection a priority", Bangkok Post, https://www.bangkokpost.com/tech/1685992/thaicert-moving-to-ncsa-under-new-law (accessed on 4 May 2020). [36]

NSO (2019), "Big data application in Thailand's government", National Statistical Office, Bangkok, https://unstats.un.org/bigdata/events/2019/hangzhou/presentations/day3/5.%20Big%20Data%20Application%20in%20Thailand%E2%80%99s%20Government.pdf. [8]

OECD (2021), *Good Practice Principles for Data Ethics in the Public Sector*, OECD, Paris, https://www.oecd.org/gov/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.htm. [27]

OECD (2020), "OECD Digital Government Index (DGI): 2019"*, OECD Policy Papers on Public Governance*, No. 3, https://www.oecd.org/gov/digital-government/oecd-digital-government-index-2019.htm. [5]

OECD (2020), "The OECD Digital Government Policy Framework: Six dimensions of a Digital Government"*, OECD Public Governance Policy Papers*, No. 02, OECD Publishing, Paris, https://doi.org/10.1787/f64fed2a-en. [3]

OECD (2019), "Data in the digital age"*, OECD Going Digital Policy Note*, OECD, Paris, http://www.oecd.org/going-digital/data-in-the-digital-age.pdf. [10]

OECD (2019), *The Path to Becoming a Data-Driven Public Sector*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/059814a7-en. [1]

OECD (2017), *Trust and Public Policy: How Better Governance Can Help Rebuild Public Trust*, OECD Public Governance Reviews, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264268920-en. [23]

OECD (2016), *Open Government: The Global Context and the Way Forward*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264268104-en. [26]

OECD (2014), *Recommendation of the Council on Digital Government Strategies*, OECD, Paris, http://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf. [2]

OECD (2013), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. [32]

OECD/ADB (2019), *Government at a Glance Southeast Asia 2019*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264305915-en. [16]

ONDE (2020), *About ONDE: Vision*, Office of the National Digital Economy and Society [11]

Commission, Bangkok, https://www.onde.go.th/view/1/Vision/EN-US.

ONDE (2019), "Open and connected governance in Thailand", Presentation by Dr Piyanuch Wuttisorn, Secretary General, Office of the National Digital Economy and Society Commission (ONDE), in the context of the OECD Open and Connected Review of Thailand. [37]

ONDE/MDES (2019), *Digital Thailand: Policy and initiatives*, Unpublished (distributed during OECD mission to Bangkok), Office of the National Digital Economy and Society Commission, Bangkok. [12]

Rohaidi, N. (2019), "Airada Luangvilai, Senior Executive Vice President, Digital Government Development Agency, Thailand: Women in GovTech special report", *GovInsider Asia*, https://govinsider.asia/data/airada-luangvilai-senior-executive-vice-president-digital-government-development-agency-thailand-women-in-govtech-special-report-2019/. [19]

Segkhoonthod, S. (2017), "Digital government and digital public services", Electronic Government Agency and Thailand Digital Government Academy, Bangkok, https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2017/Sep-SCEG2017/SESSION-1_EGA_Dr_Sak_Sekhonnthod.pdf. [24]

Stats NZ (2019), *Data Ethics Advisory Group*, https://www.data.govt.nz/about/government-chief-data-steward-gcds/data-ethics-advisory-group/ (accessed on 3 May 2020). [29]

Thiratitayangkul, C. (2019), "Open and digital government", Presentation in the context of the OECD mission to Bangkok, Thailand, 3 April 2019. [21]

Tortermvasana, K. (2018), "Big data panel to direct country's digital transition", *Bangkok Post*, https://www.bangkokpost.com/business/1420115/big-data-panel-to-direct-countrys-digital-transition (accessed on 22 April 2020). [15]

Ubaldi, B. (2013), "Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives", *OECD Working Papers on Public Governance*, No. 22, OECD Publishing, Paris, http://dx.doi.org/10.1787/5k46bj4f03s7-en. [17]

Ubaldi, B. et al. (2019), "State of the art in the use of emerging technologies in the public sector", *OECD Working Papers on Public Governance*, No. 31, OECD Publishing, Paris, https://doi.org/10.1787/932780bc-en. [33]

US Government (2020), *2020 Action Plan*, Federal Data Strategy – Leveraging Data as a Strategic Asset, https://strategy.data.gov/action-plan/. [13]

van Ooijen, C., B. Ubaldi and B. Welby (2019), "A data-driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance", *OECD Working Papers on Public Governance*, No. 33, OECD Publishing, Paris, https://dx.doi.org/10.1787/09ab162c-en. [4]

Welby, B. (2019), "The impact of digital government on citizen well-being", *OECD Working Papers on Public Governance*, No. 32, OECD Publishing, Paris, https://dx.doi.org/10.1787/24bac82f-en. [22]

From:

Open and Connected Government Review of Thailand

Access the complete publication at:

https://doi.org/10.1787/e1593a0c-en

Please cite this chapter as:

OECD (2022), “Enabling a data-driven public sector”, in *Open and Connected Government Review of Thailand*, OECD Publishing, Paris.

DOI: https://doi.org/10.1787/2ab0c605-en

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area. Extracts from publications may be subject to additional disclaimers, which are set out in the complete version of the publication, available at the link provided.