5 Conclusions

Data driven public sector policies represent a paradigm shift for administrations with regard to the management and ethical use of data, resulting in the need for a comprehensive policy approach to create public value based on data assets. This chapter presents key findings and policy recommendations for public administrations to support the successful implementation of data driven public sector policies.

Based on the OECD's analysis of how countries are using data, and the gaps that exist between their ambitions and the reality, this report has proposed three areas for countries to focus on in their quest towards a data-driven public sector. Together, these inter-connected areas address the need for creating the foundations for a value-oriented and trustworthy application of data in the public sector.

In order to extract and deliver value from data, governments must build a solid data governance foundation. Such a foundation should allow coherent policy implementation, and define trustworthy and safe environments for the ethical sharing and reuse of data.

Data governance is a growing priority across OECD member and partner countries. Ensuring a holistic approach to data governance that reflects the strategic, tactical and delivery needs; focuses on how the use of data can generate public value; and enshrines the rights of citizens in conversations about the use of data can help to successfully advance the principles and practices of a data-driven public sector (DDPS). The need for public sector data governance is built on three premises:

1. **Joining up government as a whole**, thus ensuring greater coherence when moving towards the construction of a data-driven public sector.
2. **Enabling government as a platform**, to help improve the delivery of proactive and user-driven public services, and promote the development and adoption of common tools for greater data integration within and outside the public sector (e.g. cross-sector and cross-border data sharing) as well as collaboration with non-governmental actors.
3. **Building greater trust in government** (e.g. to ensure the trustworthy, ethical and transparent processing of data) by ensuring that data initiatives and practices respect, and are in line with, citizens' digital rights.

This is particularly important as the fast-paced proliferation of data-driven initiatives across the public sector can lead to fragmented efforts and set the basis for new legacy challenges in the future. Data governance can help prevent and address these challenges and create the right context for the application of data for greater public value in a coherent fashion.

At the national level, OECD member and partner countries are moving towards **national data strategies and clearer institutional leadership structures** as a means to bring together dispersed data policies, including data sharing within the public sector, open data, and data ethics and protection. At the same time, improving the technical infrastructure and architecture to facilitate data sharing implies the development of common frameworks and tools that can be easily adopted, scaled up and widespread across the public sector as a means to support coherence and integration. These efforts should be sustained.

The conceptualisation, implementation and evaluation of data governance should be open, inclusive, iterative, collective and value based.

It is important to acknowledge that data governance needs to evolve in response to the digital maturity of a society, highlighting the connection between government-wide data policies and other policy fields, such as open government and public sector innovation.

Governments should recognise the opportunities that exist to engage the public, collaborate with non-governmental actors including researchers and academia, and stimulate private sector investment. They should make every effort to bring together public servants, civil society and other stakeholders to work together to design integrated policies and services that cross organisational boundaries in order to meet the end-to-end need of a citizen through all their interactions with the state, and not just those which a single organisation handles.

This implies, for example, bringing key actors from all sectors on board during the development and implementation of the national data strategy. By doing so, these actors can become active agents of the transformation of government by sharing knowledge (e.g. to identify otherwise missed policy priorities and

emerging risks), capacities (e.g. talent and digital solutions through partnerships) and data itself (e.g. through community-, consent-based, trustworthy and purposeful data-sharing frameworks).

While public sector capabilities and internal dialogue on the impact and effectiveness of policy making, service delivery and performance measurement are all important, external actors need to be part of the solution, from conceptualisation to implementation and evaluation.

Although it is easy for public sector organisations to state that "data are an asset" in their data strategy, it is much harder in practice to translate it into a defined value so as to include data in asset registers or on balance sheets.

There is no simple, one-size-fits-all, solution for responding to this challenge. This leaves individual public sectors free to develop methodologies that reflect their local context to define and measure the value of data for their organisations and in their societies. Being effective in defining and measuring the value of data will help public sector organisations to understand their contribution to "public value" and communicate the purposes for which data are used and the expected benefits for society.

Recognising the government data value cycle and its policy implications, and using this knowledge as the basis for mapping the flow of data and the barriers and opportunities are paramount to unlocking the value of data.

There are practical implications for the way in which public sector organisations work together when it comes to data-driven approaches. This reflects the importance of mapping the flow of data and the integration of the data value cycle (from data generation and openness to reuse), as well as the acknowledgement that each stage entails specific policy implications (e.g. a focus on data generation and collection can help reduce biased policy action).

Public sector capability (e.g. in terms of talent, stewardship and multidisciplinary teams) and formal institutional networks can help deliver value from data.

Several countries have created roles and organisations to enhance accountability around the monitoring and transparency of data use. Public sectors can benefit from establishing recognised roles with clear career paths, as well as institutions with responsibility for stewarding the accountable application of data to generate, and preserve, public value throughout the government data value cycle. Yet, governments should also ensure that data stewardship is widespread across the public sector, at different levels and in different institutions.

Policy issues increasingly require the simultaneous attention of specialists from different domains; a diverse and multi-disciplinary team can provide a better approach to delivering a response to such challenges. Bringing together all those involved with the "anticipation and planning", "delivery", and "evaluation and monitoring" of a given policy issue will result in improved quality at each of those stages through better understanding of the user need, developing a clear purpose and increasing public value.

The DDPS approach should enable experimentation and challenge preconceived ideas and assumptions. This requires new funding models that give teams the flexibility to initiate ambitious ideas and then iterate on them. It also means committing to measuring and evaluating activity to make the argument for ongoing investment and ensuring longer term sustainability.

As countries consider the role of data from "anticipation and planning" through to "evaluation and monitoring" there are increasing opportunities to learn about the impact of policy and services on society and respond accordingly. Therefore, public sectors should encourage flexibility in funding and delivery models that encourage experimentation and speak positively about making changes in response to data, especially where it challenges initial hypotheses.

Nevertheless, being in a position to respond to the insights generated by data throughout the policy life cycle means committing to implementing measurement and evaluation mechanisms at its start, middle

and end. Defining baselines and performance methodologies is not something that can be done retrospectively. Therefore, no planning or delivery should take place without considering how activity will be evaluated, performance monitored or impact measured.

Increased data flows and sharing across borders can help deliver value to citizens. Yet, governments must ensure the right balance between ensuring the free flow of valuable datasets for policy making and service delivery and protecting sensitive and personal data.

Shared public sector data governance frameworks and data-sharing infrastructures (as observed in some Nordic countries) provide the basis for the design and delivery of cross-border services. However, the growing need for government intervention to prevent data misuse and to ensure citizens' right to control how their data are used can lead to a state of data overprotection, which can have potential negative implications in terms of public service delivery and evidenced-based policy making.

Governments need to find the right policy arrangements (and the deployment of the relevant data tools to support their implementation) to ensure the secured transfer of data and promote the delivery of value for citizens in a trustworthy fashion.

Public sectors need to ensure data are handled in an ethical manner, data privacy is protected and consent respected, transparency of data is clear and accessible, and digital security is taken into account. This implies enabling the right data governance frameworks and environments to ensure the trustworthy management and processing of data across the data value cycle.

Trust is indeed essential to increase individual and collective well-being. As governments gradually turn to data to build trust from citizens, the way data are handled becomes a priority. As a result, several OECD countries have placed a high priority on ethics, privacy and consent, transparency, and security. When appropriate, public sectors should develop and/or update legal and regulatory frameworks to respond to the current needs in terms of digital rights and citizens' trust in government.

These challenges can be met by either promoting ethical behaviour through an independent body for government-held data or through ethical frameworks, which are not intended to be prescriptive but aim at widening a common understanding and working through ethical concerns.

Since an unethical situation is not necessarily unlawful, there is an important need to establish a responsible value-based environment and guidelines in order to retain citizens' trust.

In response to challenges around the use of data and public trust, the OECD Thematic Group on Data-driven Public Sector developed a set of proposed ethics guidelines aiming at promoting responsible and ethical behaviour among public servants handling data. While covering the four areas of ethics, privacy and consent, transparency, and security, the guidelines are not meant to be prescriptive, as no two countries are the same. Instead, governments should use the guidelines as suggestions and tailor them to their own needs.

The increasing use of artificial intelligence in government to improve decision making and service delivery makes the transparency of data and algorithms essential. Openness and clarity in terms of what data are used, for what purpose and by whom should remain a priority for governments.

Transparency of data use helps build trust, as this discloses the purpose of data collection and the way it is being used. Public trust is also strengthened by people clearly understanding the intended goal and output of data used for algorithmic decisions and by governments making their performance public. Public sectors should promote transparency by giving more details not only about the purpose and processing of data, but also about the decision-making algorithm, and by publishing government performances.
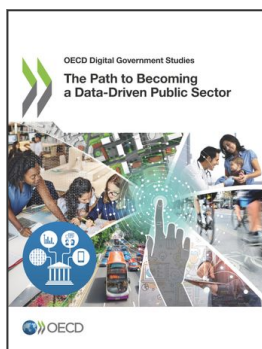
The OECD has developed its own set of principles on artificial intelligence, which were adopted in May 2019 and aim at promoting artificial intelligence that is innovative and trustworthy and that respects human rights and democratic values.

Governments should include digital security either in a stand-alone strategy or on the country's broader policy agenda, with an emphasis on closing the digital security skills gap.

All efforts put in place to secure data protection should be taken more seriously than ever. Digital attacks can be extremely costly, not only in terms of financial cost, but also in terms of reputation. An organisation suffering from a data breach can lose its users' trust, as well as the trust of potential users.

The increasing number of sophisticated hackers also needs to be addressed, starting by equipping the public with digital security skills. Digital security should not compensate for the lack of skills or capacity, instead equipping citizens to understand how to keep themselves safe, and consequently to be savvier in their online interactions and the use of their personal information, is essential in the digital age.

Digital security is therefore not an optional extra, but needs to be a fundamental part of government's digital, data and technology strategies. It needs to be addressed by government-wide strategies and be approached in ways that enable the proactive use of data for designing and delivering better quality government.