OECD Digital Government Studies

The Path to Becoming a Data-Driven Public Sector

OECD

OECD Digital Government Studies

The Path to Becoming a Data-Driven Public Sector

Please cite this publication as:
OECD (2019), *The Path to Becoming a Data-Driven Public Sector*, OECD Digital Government Studies, OECD Publishing, Paris, *https://doi.org/10.1787/059814a7-en*.

ISBN 978-92-64-51795-0 (print)
ISBN 978-92-64-62527-3 (pdf)

OECD Digital Government Studies
ISSN 2413-1954 (print)
ISSN 2413-1962 (online)

Photo credits: Cover © Baseline Arts.

Corrigenda to publications may be found on line at: *www.oecd.org/about/publishing/corrigenda.htm*.

Foreword

As rapid digital transformation changes all aspects of daily life, citizens expect their governments to provide better services and policies that deliver on the promises of the digital age. Advances in technology and data-driven approaches can radically change the way governments and citizens interact. Through a strategic use of data, governments can create conditions for improving the quality of public services, increasing the effectiveness of public spending and safeguarding ethical and privacy considerations. A data-driven public sector requires governance mechanisms that favour efficient data handling but also preserve public trust when using data to deliver outcomes.

The OECD is a long-standing advocate of a data-driven approach; the *2014 OECD Recommendation of the Council on Digital Government Strategies* recognises the central importance of data in the shift to digital government. This report describes trends, opportunities and challenges for policy makers in the use of data as a strategic asset. It highlights country practices and provides guidance on applying data to improve the quality of public services and citizen well-being.

This report addresses three areas of discussion: the importance of data governance as the foundation of a data-driven public sector, the use of data to increase public value, and the role of data in building public trust.

Data governance underpins the readiness of the public sector to adopt data-driven approaches. Governments can then use data not only to anticipate the public's needs, but also to deliver better services, improve policy implementation and evaluate their own performance. Nevertheless, the increasing use of sensitive or personal data raises new challenges for governments. This report explores ongoing efforts to ensure ethical, transparent and secure ways of managing and handling data to support public trust.

The report is the culmination of OECD work on digital government and open government data, which seeks to support governments in using data to transform the public sector and address issues of public governance. This work is grounded in the 2014 OECD Recommendation and carried out under the auspices of the OECD Working Party of Senior Digital Government Officials. The report builds on the work of the Working Party's Thematic Group on the Data-Driven Public Sector, the OECD Working Paper *A data-driven public sector*, and the analysis from OECD Digital Government Reviews. Finally, it reflects the specific experiences of Denmark, Ireland, Korea, Portugal, Sweden and the United Kingdom.

This report, as document GOV/PGC(2019)50, was approved by the Public Governance Committee at its 60th session on 15 November 2019, and was prepared for publication by the OECD Secretariat.

The data-driven public sector framework presented in this report can be used by countries or organisations to assess the different elements required for using data to make better-informed decisions across the public sector. It is not intended as a one-size-fits-all prescriptive model, but is offered as a tool to support the development of additional case studies to foster data-driven approaches in different policy areas.

Acknowledgements

This report was prepared by the OECD Directorate for Public Governance, under the leadership of Marcos Bonturi. It was produced by the OECD Reform of Public Sector Division, under the supervision of Barbara-Chiara Ubaldi, Acting Head of Division and Head of the Digital Transformation of the Public Sector work.

Chapters 1 and 3 were written by Benjamin Welby, Digital Government Policy Analyst. Chapter 2 was written by Jacob Arturo Rivera Perez, Digital Government and Open Data Policy Analyst. Chapter 4 was written by Lucia Chauvet, Junior Consultant. The case studies were written by Gavin Ugale with input from Dr. Michael Nest, consultant, on fraud in social benefits programmes, and research support by Alexis Bernigaud (Public Sector Integrity); and Seokhee Lee, Natalia Nolan Flecha and Daniel Gerson (Public Employment and Management). Piret Tonurist, Policy Analyst, Public Sector Innovation, and Cecilia Emilsson, Junior Consultant, contributed to Chapter 2.

The OECD Secretariat is also thankful to Bas Groenveld, Adviser on International Affairs, Dutch Ministry of the Interior and Kingdom Relations; Sam Roberts, Senior Policy Adviser, Data Policy Team, Department for Digital, Culture, Media and Sport, United Kingdom; Claire Chapman, Office for Artificial Intelligence, United Kingdom; and Harry Armstrong, Head of Technology Futures, Nesta, for the support provided for the finalisation of Chapter 2.

All chapters benefitted from the strategic orientation and revisions of Barbara-Chiara Ubaldi. Benjamin Welby served as the lead co-ordinator of the report. Colleagues from within the OECD, including Janos Bertok, Klas Klaas, Edwin Lau and Stéphane Jacobzone, reviewed and provided comments. Editorial support was provided by Jennifer Allain and Liv Gaunt.

This report builds on the body of work produced by Jacob Arturo Rivera Perez, Reginald Dadzie and Cecilia Emilsson in the OECD *Open Government Data Report,* and the working paper on a “A data-driven public sector” written by Charlotte Van Ooijen, Barbara Ubaldi and Benjamin Welby. The OECD is also grateful for the early support of the governments of Denmark, Ireland, Korea, Portugal, Sweden and the United Kingdom; the comparative data collection referenced throughout this report was made possible by their contributions.

The OECD wishes to acknowledge the ongoing support of the OECD Working Party of Senior Digital Government Officials (E-Leaders) and the OECD Expert Group on Open Government Data to the data-driven public sector agenda, with particular thanks to the Data-driven Public Sector Thematic Group led by the Netherlands and benefitting from the input of Argentina, Chile, Colombia, Denmark, Egypt, Estonia, the European Commission, Israel, Italy, Latvia, Luxembourg, Panama, Portugal, Slovenia, Spain, the United Kingdom and Uruguay.

Table of contents

Tables

Figures

Boxes

Executive Summary

The rise of data and digital technologies are rapidly transforming economies and societies, with enormous implications for governments' daily operations. Twenty-first century governments must keep pace with the growing expectations of their citizens, manage increasing pressure on their budgets and react to new policy challenges. Any failure to adapt to this new and changing environment could expose them to damaging risks and a consequent diminishing of public trust.

Data has the potential for playing a positive role in society. But, despite some advances, turning the promise of data into tangible, measurable and consistent outcomes remains largely elusive. In the public sector, the role of data in the ongoing digital transformation has come up against legacy technologies, skills shortfalls and legal obstacles. Some countries have made significant progress in strengthening the capacity to use data strategically to improve policy making, service delivery or performance management. Individual organisations have also produced impressive results. Nevertheless, the use of data is not yet viewed -- or resourced – as a fundamental means of creating public value

Building on previous OECD work about the role of data in society and the economy, this report proposes a model for understanding the 'data driven public sector' (DDPS) that will maximise the opportunities provided by twenty-first century data. It proposes that a truly data-driven public sector:

- recognises data as a key strategic asset with its value defined and its impact measured
- reflects active efforts to remove barriers to managing, sharing and re-using data
- applies data to transform the design, delivery and monitoring of public policies and services
- values efforts to publish data openly as much as the use of data between, and within, public sector organisations.

This report underlines the importance of adopting a whole-of-government approach to developing a coherent and comprehensive model of data governance that helps governments deliver better services while being efficient, transparent and trustworthy in their use of data. It does this by presenting three areas for discussion.

First, countries need to develop a comprehensive model for data governance. The report proposes a definition of data governance, establishes the purpose of data governance and describes the development of a common framework for establishing such governance. The report argues that countries need to develop a cross-government, coherent approach to data governance that underpins a truly data-driven public sector and reflects the critical elements for achieving system-wide benefits in government. The components of this framework are:

- Securing the leadership and vision to ensure strategic direction and purpose for the data-driven conversation throughout the public sector
- Encouraging the coherent implementation of this data-driven public sector framework across government as a whole and within individual organisations
- Putting in place, or revisiting, rules, laws, guidelines and standards associated with data

- Ensuring the existence of a data architecture that reflects standards, interoperability and semantics throughout the generation, collection, storage and processing of data
- Developing the necessary data infrastructure to support the publication, sharing and re-use of data.

Second, countries can apply data to generate public value through three types of activity:

- Anticipation and planning: using data in the design of policies, planning of interventions, anticipation of possible change and the forecasting of needs
- Delivery: using data to inform and improve policy implementation, the responsiveness of governments and the activity of providing public services
- Evaluation and monitoring: the use of data in measuring impact, auditing decisions and monitoring performance

The third area is the role of data in trust. Public trust in government is a critical factor in citizen well-being but is far easier to lose than to build. The way in which governments handle citizen data can be particularly damaging. The report challenges governments to:

- adopt an ethical approach to guide decision making and inform behaviour
- protect privacy, promote transparency and design user experiences that help citizens understand and grant or revoke consent for their data to be used
- approach the security of government services and data in ways that mitigate risks without blocking the transformation of the public sector

Using the DDPS framework developed by this analysis, three case studies are presented. They demonstrate that a DDPS approach is applicable to local and institutional levels Just as well as to the centre of government. These case studies consider the DDPS experience in the areas of public sector integrity, public employment and management, and budgeting and public expenditures. Countries and organisations can use the framework of this report to assess their own readiness for being a data-driven public sector.

1 Introduction

This chapter provides an overview of the importance of digital government approaches to efforts to transform countries in general before focusing on the evolving understanding of the use of data in the public sector. The chapter concludes by outlining the structure of the report and identifies the anticipated impact and opportunities that will follow.

Digital government approaches are the foundation for transforming a country

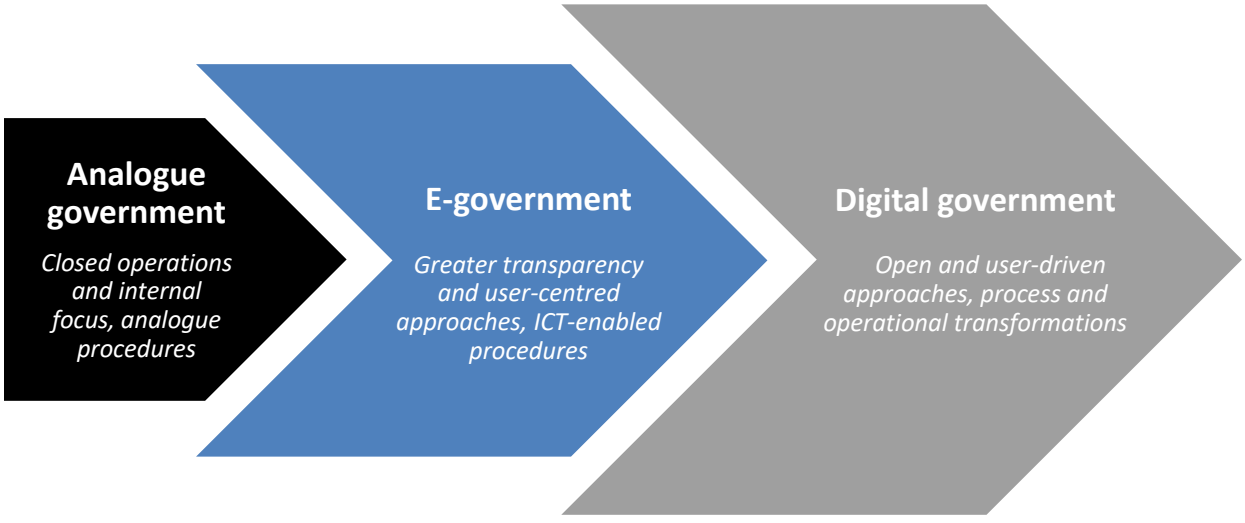
The growth of data and digital technologies are rapidly transforming economies and societies, with enormous implications for governments' daily operations. These technologies have the potential to transform mundane tasks like processing documents or routing requests, and improve service delivery, e.g. speed up diagnosis through medical imagery, automate public transport and detect criminal threats in real time.

Twenty-first century governments must keep pace with their citizens' expectations, manage increasing pressures on their budgets and respond to new policy challenges while at the same time being aware that any failure or misstep in adapting to this new and changing environment could expose them to damaging risks and a consequent diminution of citizens' trust.

The OECD's work on digital government and open government data supports governments in their ambitions for "digital transformation" (see Annex A). Through research, guidance and creating opportunities for collaboration, the OECD helps governments rethink their role, scope of activity and ways of working in light of digital technologies. This work is part of the OECD Public Governance Directorate's mandate to help countries move beyond identifying the possibilities of a particular technology to embedding its application within public sector reform agendas. The goal is to support policy design and delivery processes that reflect the opportunities for digitally native, networked societies and deliver new forms of interaction between the state and its citizens and businesses.

Realising those opportunities demands a paradigm shift in the use of digital technologies and data within governments from "e-government" to "digital government". An "e-government" approach considers technology to be the solution for digitising delivery of an existing analogue process in search of efficiency gains; it makes the implementation of technology the focus. By contrast, digital government practices see technology as secondary to a focus on meeting the need of a user by re-engineering and re-designing services and processes. This digitalisation goes hand in hand with establishing digital-by-design cultures that transform the behaviours of an organisation.

Figure 1.1. From analogue to digital government



Source: Based on OECD (2014[1]) *Recommendation of the Council on Digital Government Strategies OECD,* https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406.

The desire to use digital technologies and data to foster more open, innovative and efficient public sectors is behind the development of the OECD *Recommendation of the Council on Digital Government Strategies* (OECD, 2014[1]). Through the Recommendation, the OECD has identified several important conditions for successful digital transformation. These have been endorsed by the 36 OECD countries as well as a further 10 non-member countries which have adhered to the Recommendation.[1] This transition is not simply about the application of technology to support government functions, but an evolution in how governments consider the needs of their citizens and involve the public as participants, rather than solely as beneficiaries. This means moving away from top-down assumptions about citizens' and businesses' needs and creating ways to empower them to work with government to identify and understand those needs as well as collaborating to address them. This process should result in governments creating opportunities to improve citizens' well-being by being increasingly responsive, protective and trustworthy (Box 1.1).

Box 1.1. The impact of digital government on citizens' well-being

Countries that commit to a digital government agenda can improve outcomes for their citizens by using digital, data and technology to support the following efforts to become more responsive, protective and trustworthy.

- Responsive governments…
  - … involve people throughout the design and delivery life cycle to ensure that their needs have been, and continue to be, understood
  - … proactively reach out to where people spend time (in both online and offline communities) and involve them in the design and delivery of services
  - … don't just implement technology, but design government and the end-to-end experience of services.
- Protective governments…
  - … prioritise the protection of the public from external digital security threats and ensure that provided services are reliable and secure
  - … encourage efforts to restore and distribute trust throughout digital communities
  - … think about regulation in the context of outcomes rather than an approach to specific technologies.
- Trustworthy governments...
  - … strike the right balance between online safety and democratic freedoms to build public trust and confidence
  - … deliver high-quality services that understand users and are open to challenge and feedback
  - … show citizens what government is doing and empower individuals to see, and control, how their data are being used.

Source: Welby, B. (2019[2]), "The impact of digital government on citizen well-being", https://doi.org/10.1787/24bac82f-en.

The *Recommendation of the Council on Digital Government Strategies* (OECD, 2014[1]) comprises 3 pillars and 12 principles that ensure the successful design, development and implementation of digital government strategies to enable transformation. The six dimensions of activity shown in Figure 1.2 shape the level of a country's digital government maturity.

1. **Data-driven public sector:** The importance of data as a foundational enabler for public sector organisations to work together in forecasting needs, shaping delivery, and understanding and responding to change.

2. **Open by default:** The desire of governments to collaborate across organisational boundaries, and involve those outside government is an important marker for a culture that will embrace the principles of transparency and accountability that underlie digital ways of working.
3. **Government as a platform:** Building an ecosystem to support and equip public servants to make policy and deliver services that encourages government to collaborate with citizens, businesses, civil society and others.
4. **Digital by design:** The intent of a government to approach digitalisation with an understanding of all the strategic activities needed to facilitate successful and sustainable transformation by changing the processes and culture of delivery.
5. **User-driven:** An approach to delivery enabled by an open culture and supported by ambitions of digital by design to include, and be led by, the needs of the public rather than the assumptions of government.
6. **Proactive:** The ability of governments to anticipate, and rapidly respond to, the needs of their citizens through the application of the five above-mentioned dimensions. Transformed government allows problems to be addressed from end to end rather than the otherwise piecemeal digitisation of component parts.

Figure 1.2. The main characteristics of a digital government

Source: OECD (forthcoming[3]), *Digital Government Indicators*

The focus of this report is the "data-driven public sector" (DDPS). However, it is important to recognise that DDPS is one of six dimensions that, taken collectively, underpin successful implementation of digital government approaches.

Towards a data-driven public sector

There have been ambitious statements over the last decade about the potential economic and societal opportunities for exploiting data. While some of those hopes have been realised, there have also been some high-profile examples where attitudes towards data have damaged trust in institutions. The most

notable in recent years is perhaps the role of Facebook data being used for political purposes. Turning the promise of data into tangible, measurable and consistent outcomes remains elusive.

This has been especially true within the public sector during its ongoing digital transformation, where legacy technologies, capability gaps and legal obstacles have slowed progress. Nevertheless, there has been a growing recognition of the importance of data to underpin, shape and inform the activity of the public sector at large. Some efforts have focused on the role of open government data (OGD) with the resulting publication of datasets to stimulate private sector innovation, provide opportunities for the economy at large and increase government accountability. Other efforts have looked at the internal application of data to create value and equip public servants to use data in their work. The opportunities associated with emerging technologies such as artificial intelligence and distributed ledgers have also highlighted new challenges around questions of data quality, rights and ethics (van Ooijen, Ubaldi and Welby, 2019[4]; Berryhill, Bourgery and Hanson, 2018[5]; Ubaldi et al., 2019[6]).

Some countries have made significant progress and individual organisations have seen impressive data-driven results while initiatives like the Digital Nations Data 360° Declaration (2019[7]) show increasing attention being given to this agenda. However, governments have not yet managed to create coherent and consistent conditions at either the centre of government, or within individual public sector organisations, for data to be viewed and resourced as foundational for creating public value through improved policy making, service delivery and performance management.

This report describes how data-driven approaches can support public sectors to be more open, innovative and agile. The challenge facing governments in maximising the opportunities of a DDPS is in creating the right conditions and facilitating the right behaviours such that there is a whole-of-public sector competence and coherence to the data agenda. A truly data-driven public sector:

- recognises data as a key strategic asset, defines its value and measures its impact
- reflects active efforts to remove barriers to managing, sharing and reusing data
- applies data to transform the design, delivery and monitoring of public policies and services
- values efforts to publish data openly and the use of data between and within public sector organisations
- understands the data rights of citizens in terms of ethical behaviours, transparency of usage, protection of privacy and security of data.

Governments that have implemented a strategic approach for the use of data throughout the public sector are better able to anticipate societal trends and needs and consequently develop more effective long-term plans. Additionally, the active use of data plays an important role in the ongoing design and delivery of public services and efforts to analyse and evaluate all types of government activity to allow for continuous improvement. It also offers transparency about success and failure in ways that support accountability and stimulate public engagement and trust.

It is fundamental for governments to recognise that embracing a DDPS approach is about creating the right conditions within government to provide data-related leadership, develop talent and build skills throughout the public sector. This includes the full gamut of government actors (in budgeting, public employment, regulation, public sector integrity, etc.) as well as in sector-specific interventions such as education, health and welfare.

Furthermore, a DDPS approach seeks to combine conversations around OGD and internal government data so that they are understood collectively rather than as two separate agendas. OGD is an important part of the conversation, but should no longer be treated as an isolated policy. Instead, it is simply data, whether open or closed, that can result from good public sector data management practices and policies as presented in this report. Balancing open-by-default approaches with the protection of sensitive and private data, data ethics, and citizens' consent are equally important in securing the promise of the DDPS.

The link between the use of data and a whole host of public sector outcomes is critical. Many aspects of public sector delivery are based on hypotheses about the efficacy of government interventions; data allow governments to test and adjust their approaches. In the field of regulation, to cite one example, the ability to carry out real-time analysis based on various sources of data provides a transformative opportunity to rethink from the ground up the way in which a particular aspect of the public sector might function, thus moving away from a one-size-fits-all model to responding to demand, risk and context (OECD, 2018[8]).

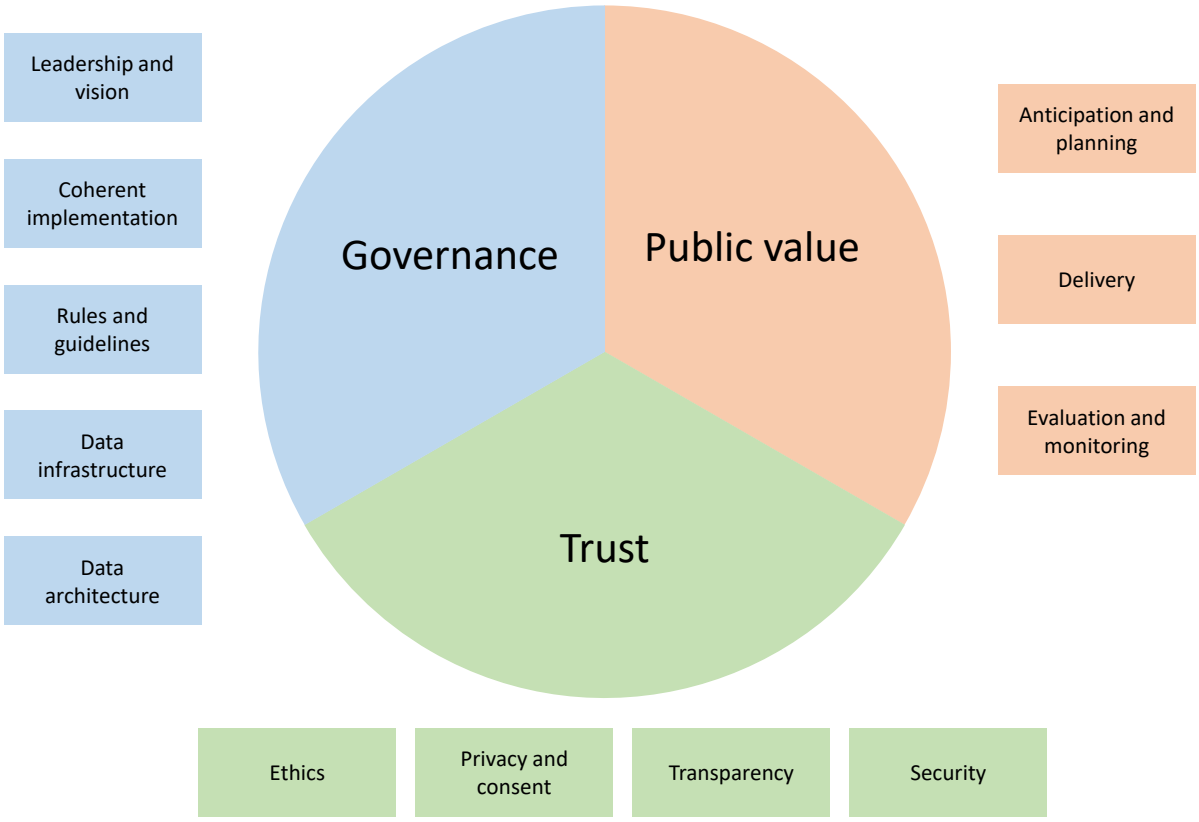
It is important to keep in mind the role which internal attitudes towards risk management play in the ability to embrace new and emerging technologies. A DDPS enables the effective use of emerging technologies such as artificial intelligence and distributed ledgers, among others. This report lays out the need for a coherent and comprehensive data governance model that provides a framework to build trust, mitigate risk, and encourage governments to experiment and innovate. Nevertheless, while leadership and vision are important, there remains a critical need to consider closing the data-related skills deficit within the public sector.

The data-driven public sector report

This report reflects on the evolution of understanding about the trends, opportunities and challenges that emerge within data-driven public sectors and provides evidence and guidance for countries seeking to embrace all the opportunities such a model might offer. It provides a conceptual framework to support countries in their efforts to understand the value of data for the public sector and to develop a strategic approach to capturing this value.

The analytical framework used to consider the full breadth of DDPS consists of the following three areas of focus: 1) a comprehensive model for data **governance** (see Chapter 2); 2) the application of data for **public value** (see Chapter 3); and 3) the role of data in public **trust** (see Chapter 4). Within these 3 areas, a further 12 sub-dimensions are proposed, not to represent an argument for a one-size-fits-all model, but to acknowledge it is the combination of efforts across these areas that will support attempts to implement a DDPS as shown in Figure 1.3. This is an aspirational model composed of best practices from around the world. No country has yet implemented a holistic approach to this topic.

Figure 1.3. The 12 facets of a data-driven public sector



Chapter 2 looks at data governance and seeks to answer the question: what does a country need to put in place to create the enabling conditions for a DDPS? It proposes a definition of data governance, establishes the purpose of having data governance and talks through the development of a common framework for establishing such governance. The report will argue that countries need to develop a cross-government, coherent approach to data governance that broadens the usual conversation on this topic to reflect the critical elements for achieving system of government-wide benefits in underpinning a truly data-driven public sector. The elements of this framework are:

- the leadership and vision to ensure strategic direction and purpose for the data-driven conversation throughout the public sector
- the need for coherent implementation across government as a whole and within individual organisations
- putting in place, or revisiting, rules, laws, guidelines and standards associated with data
- developing the necessary data infrastructure to support the publication, sharing and reuse of data
- having a data architecture which reflects standards, interoperability and semantics throughout the generation, collection, storage and processing of data.

Chapter 3 focuses on how the application of data generates public value. After a discussion about the government data value cycle and the ways in which countries might define and measure “public value”, the chapter considers how such value might be created, or increased, through three types of activity:

1. Anticipation and planning: The role of data in enabling the design of policies, planning of interventions, anticipation of possible change and forecasting of needs.

2. Delivery: How the use of data can inform and improve the implementation of policy, responsiveness of government and provision of public services.
3. Evaluation and monitoring: The approach to data involved in measuring impact, auditing decisions and monitoring performance.

These uses of data are not separate silos, but highlight that different aspects of government reflect different parts of the design, delivery and implementation lifecycle, from planning for the future to delivering today and evaluation of what has already happened. Each of these aspects informs and shapes the next aspect in ways that support an iterative, continuously improved approach to the effectiveness and efficiency of government.

Putting in place good data governance and applying data to create public value will increase the well-being of citizens by delivering better quality services that are more inclusive of, and responsive to, citizens' needs. However, one of the strands of citizen well-being has a less tangible source, and that is public trust in government. The trust of citizens in government is far easier to lose than it is to build, and can be damaged by the way in which governments handle their citizens' data. Therefore, Chapter 4 looks at how a DDPS can respond to these challenges and the data rights of citizens by:

- adopting an ethical framework to guide decision making and inform behaviour
- protecting privacy and clarifying data ownership and permissions while understanding the dynamics and user experience of how citizens understand and grant or revoke consent for data to be used
- securing transparency in how data are used
- recognising that to mitigate risks, the security of government services and data must be considered in ways that do not impede efforts to transform the experience of the public or the capacity of public servants to deliver.

In presenting the facets of a DDPS discussed above and summarised in Figure 1.3, this framework can inform the political leadership and strategy either for the centre of government, or for the local context within a given sector or organisation. This report is accompanied by two case studies looking at the DDPS experience in the areas of public sector integrity, and public employment and management.

Anticipated impact and next steps

This report shows the importance of considering a whole-of-government approach to developing a coherent and comprehensive model of data governance in order to create the necessary conditions for ensuring that the benefits of data are maximised by governments being efficient, transparent and trustworthy.

This report is aspirational. It provides an overview of the state of data-driven practices in several countries. It also introduces various topics and considerations for understanding the potential of data in the public sector. This conceptual analysis results in the 3 pillars and 12 dimensions of a framework that can be used by countries and organisations for assessing the different elements required for a DDPS as shown by the recent *Digital Government Review of Panama* (OECD, 2019[9]).

While not a one-size-fits-all prescriptive model, it can inform a country's strategic efforts to move towards becoming a DDPS. Through the analysis of data governance, it will propose the main changes that countries may need to make. It will also identify the potential benefits of a DDPS in terms of the management and use of data for the design, delivery and monitoring of public policies and services. Additionally, the report will highlight the factors to take into consideration in terms of the increasing need to approach the use of data in ways that protect and enhance trust.

No country has yet addressed all of these elements. While this report could be useful to a range of different audiences, from the novice to the expert, its ambition is to provide those with the responsibility for leading

and developing data strategies with a framework that they can use to consider each of the areas that collectively will lead to digital transformation. The report will provide not only evidence for clarifying the political imperative, but also for developing business cases to support the implementation and use of data in proactive and preventative risk management, public sector productivity, and public sector innovation.

This report provides a series of conclusions that could form the basis for the development of a new OECD Recommendation setting out the practical steps that countries need to take in order to become truly data-driven and unlock the opportunities for transforming society by increasing the effectiveness of delivery, openness of engagement and trustworthiness of government.

References

Berryhill, J., T. Bourgery and A. Hanson (2018), "Blockchains unchained: Blockchain technology and its use in the public sector", *OECD Working Papers on Public Governance*, No. 28, OECD Publishing, Paris, http://dx.doi.org/10.1787/3c32c429-en. [5]

Digital Nations (2019), *Digital Nations Data 360° Declaration*, https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/documentos/noticias/Declaration%20for%20D9%20Data%20Alliance.pdf. [7]

OECD (2019), *Digital Government Review of Panama: Enhancing the Digital Transformation of the Public Sector*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/615a4180-en. [9]

OECD (2018), *The Regulatory Future of Emerging Technologies - A Scoping Paper on Gaps and Opportunities*, OECD Publishing, Paris. [8]

OECD (2014), *Recommendation of the Council on Digital Government Strategies*, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406. [1]

OECD (forthcoming), *OECD Digital Government Indicators*, OECD, Paris, forthcoming. [3]

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, http://dx.doi.org/10.1787/932780bc-en. [6]

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, http://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, http://dx.doi.org/10.1787/24bac82f-en. [2]

Note

1. The non-member countries that have adopted the Recommendation are Argentina, Brazil, Colombia, Costa Rica, Egypt, Kazakhstan, Morocco, Panama, Peru and the Russian Federation.

2 Data governance in the public sector

This chapter presents how OECD countries are moving towards the definition and implementation of holistic public sector data governance practices at the national level. It discusses the main trends and challenges observed in relation to data governance and proposes a public sector data governance framework drawing upon OECD best practices. The chapter then applies the model to provide a brief overview of data governance practices across OECD member and partner countries.

Introduction

In the early 2000s, tech giants such as Facebook realised how digital platforms and the 24-7 connected citizen provided the ideal context to collect and reuse data for business purposes. This opened a window of opportunity to start selling data-driven products and services to any company and individual with an interest in designing ad hoc marketing and communication strategies – from businesses to politicians.

Data collected through multiple sources (from mobile phones to smart home devices) are now analysed to better understand users and target potential customers, or service users. These insights are used to drive citizens' choices, increase business revenues, influence public vote, or design and deliver better services. There is a plethora of technical solutions used for this purpose (e.g. artificial intelligence [AI], big data, customer relationship management), which places the access to and sharing of data (EASD) as a precondition for data analysis techniques to help increase the value that is created for companies and shareholders.

Since The Economist published the article, "The world's most valuable resource is no longer oil, but data" in 2017 (The Economist, 2017[1]), "data is the new oil" became the new buzz phrase, and was sometimes abused and misunderstood by data enthusiasts. While this data-oil analogy aimed at increasing public awareness in response to raising data monopolies and controlled data flows, it also helped to stress how new technologies and data could help organisations to take better decisions and increase business intelligence.

Still, while the discourse on "data as an asset" is well accepted nowadays, organisations, including from the public sector, often fail to govern, manage and value data in the same way as the other assets that are relevant for their success. This undermines the possibility of taking advantage of the opportunities brought by the "datisation of a huge amount of information that was previously intangible" (Chiesa, 2019[2]).

Enabling the right cultural, policy, legal, regulatory, institutional, organisational, and technical environment is necessary to control, manage, share, protect and extract value from data. Yet, organisations from the public and private sector often face legacy challenges inherited from analogue business models, ranging from outdated data infrastructures and data silos to skill gaps, regulatory barriers, the lack of leadership and accountability, and an organisational culture which is not prone to digital innovation and change.

New challenges have also arisen resulting from citizens' data misuse and abuse cases, mainly by private sector organisations. This is paired with the inability of governments to take proactive action, keep up with technological change, and understand the policy implications of data in terms of trust and basic rights (see Chapter 4).

Responding to these challenges requires greater understanding, structure and knowledge-sharing in relation to how OECD countries address data governance in the public sector. This is well recognised by private sector actors, but is only gaining traction in the government sphere.

This chapter presents a brief overview of how national governments across OECD member and partner countries are increasingly addressing data governance as a whole, or have worked on developing specific elements of it. The chapter also presents a proposed model for data governance in the public sector, based on OECD good practices on data management and sharing within the public sector, open government data and digital government. While not exclusive, the elements presented in the data governance model guide the analytical work of this chapter.

The case for good data governance in the public sector

Good data governance can contribute to setting a common vision; enhancing coherent implementation and co-ordination; and strengthening the institutional, regulatory, capacity and technical foundations to better control and manage the data value cycle, i.e. collect, generate, store, secure, process, share and reuse data, as means to enhance trust and deliver value (see Chapter 3).

Good data governance is imperative for governments that aim to become more data driven as part of their digital strategy. It can help to extract value from data assets, enabling greater data access, sharing and integration at the organisational level and beyond, and increasing overall efficiency and accountability. However, while the concept is not new, most OECD governments are struggling to put it into practice.

The OECD has observed the following trends in the governance, management and sharing of public sector data:

> *a) Data governance is increasingly relevant to data protection practices at the global scale in a more exclusive and explicit fashion. Yet, a strong and unbalanced approach to data overprotection can reduce the value of data sharing, such as in the delivery of cross-border public services.*

Recently, data misuse by private companies and increasing concerns from citizens about data management in the public sector has triggered government intervention to improve the protection of personal data (OECD, 2019[3]). As a result, the ethical and transparent use of data is now high on the political agenda (see Chapter 4).

Data flows have increased across organisations, sectors (e.g. business-to-government) and borders, adding another level of complexity to data governance in a globalised and interconnected world. Data governance is no longer a matter limited to organisational boundaries, but a multinational concern resulting from cross-border data sharing.

In this context, international instruments such as the EU General Data Protection Regulation have sought to "give back to citizens the control over their own data" (OECD, 2019[3]), and take cross-national action to prevent data misuse. The General Data Protection Regulation pushed the data protection agenda forward, thus underlying the need for common frameworks to ensure the protection of data across borders. Nevertheless, data overprotection can result from the misunderstanding of national and international regulations and drive change in terms of policy approaches (e.g. from openness by default to "open if possible, protected if needed"[1]).

The global challenge at this stage is thus to ensure the right balance between free data flows and data protection, as stated by Japan's Prime Minister Abe during his keynote speech at the World Economic Forum in January 2019[2] (Japanese Government, 2019[4]).

> *b) Data governance elements are often in place as part of broader digital transformation policies. However, these components can be fragmented, thus reducing their whole-of-government value in terms of public sector integration and cohesion. A holistic data governance can help to join up government as a whole.*

While OECD countries have often defined elements relevant to public sector data governance in the context of digital government, open data, data management, and/or AI strategies and/or policies, these elements are often fragmented. In some scenarios, this disconnection is deeply rooted in the intricate governance arrangements supporting those policies (e.g. different public sector organisations leading these policies or lack of clarity in terms of leadership and responsibilities), therefore posing important barriers for data integration and sharing.

A holistic data governance can also help in enabling **Government as Platform** (one of the key dimensions of a digital government) (see Chapter 1). For instance, the development of common but flexible data tools (e.g. data sharing platforms) provide solutions that can be re-used across the broad public sector. At a more technical level, fragmentation also results from legacy challenges in terms of what organisation

generates and controls the data and the impossibility of sharing and accessing those data in light of specific legal arrangements, leading to siloed policy and technical solutions that add to the impossibility of building an integrated and connected government. The lack of an overarching data governance model can lead to the proliferation or duplication of data standards and technical solutions for data sharing, thus hindering data interoperability across different organisations and sectors, and affecting the possibility of integrating data, processes and organisations. It could also lead to multiple requests for citizens to provide the same personal data multiple times to the public sector unnecessarily.

A data governance framework must ensure the proper management of data through its entire life cycle (Ghavami, 2015[5]). For instance, in the past years, the open government data movement allowed for a more in-depth discussion of the need for strengthening data leadership and stewardship within the public sector. This also opened a more technical discussion on improved data management practices, e.g. around the production, storing, processing and sharing towards higher data openness. Nevertheless, these elements were not understood as part of broader public sector data efforts connecting all stages of the data value cycle (see Chapter 3). Countries suddenly realised the value of cataloguing data for openness and discoverability purposes, but have failed to acknowledge how these initiatives also had relevant policy benefits for productivity within the public sector.

On the other hand, in some OECD countries, a well-established culture of public sector efficiency led to the development of data registers as a means to improve inter-institutional data sharing. Yet, this mind-set overshadowed the growing value of opening up government data and engaging and collaborating with external actors to find solutions to policy challenges. As a result, those countries that once led the former e-government movement (with a strong focus on efficiency) lagged far behind those that doubled efforts to make share and open up data to users as means to promote business and social innovation.

OECD countries such as **Canada**, **Ireland**, the **Netherlands**, **United Kingdom** and the **United States** have moved or are moving towards the definition of overarching data strategies as means to build greater public sector cohesion and promote the integration of policies and tools.

These strategies comprise most, if not all, stages of the government data value cycle (from data production and its protection to data openness and reuse) (see Chapter 3). Still, each stage requires specific arrangements, as they produce specific policy benefits (e.g. open data enables the use of data as a platform for greater user engagement and collaboration, and better data collection production practices can help in reducing policy bias).

> *c) Policy makers can misunderstand data governance as the exclusive responsibility of IT departments, but it also implies transformation and coherence of capacities, policies, regulatory frameworks, leadership and organisational culture. There is therefore a need for more strategic approaches to data governance in the public sector.*

The OECD has observed that a strong focus on technical issues as the primary outcome of data governance can misguide data-related policy decisions. For instance, by focusing primarily on the adoption of technological solutions such as application programming interfaces (APIs) and data standards (see the Overview of public sector data governance practices later in this chapter), rather than also enabling the adequate organisational, governance and cultural context to make those tools valuable to address policy challenges. All of these are key elements of good data governance.

In some cases, OECD countries have invested resources to define strategic roles (e.g. data stewards, chief data officers) to support data governance through the definition of a stronger institutional fabric. The establishment of these strategic roles can help in scaling and sustaining policy implementation and building greater data maturity across the public sector (OECD, 2018[6]). This has taken place either in the context of data strategies or open data policies [e.g. **Korea** and the **United States** (see the Overview of public sector data governance practices later in this chapter)]. However, in most countries, data leadership and/or stewardship are still misunderstood, thus confining data governance to the activities of the IT department

and not as a factor that can help achieve policy goals through better data management and sharing practices.

> *d) Public policies tend to overlook the benefits of data governance. There is a need for promoting data governance as a sublayer of policy arrangements. This can help to extract value from data for successful policy.*

Good data governance supports public sector reform as a whole. In this light, its application is in line with core OECD principles and guidelines in areas such as digital government (OECD, 2014[7]), open government (OECD, 2017[8]), public service leadership and capability (OECD, 2018[9]), public sector integrity (OECD, 2017[10]), public procurement (OECD, 2015[11]), regulatory policy (OECD, 2012[12]), and budgetary governance (OECD, 2015[13]).

In best-case scenarios, most or some of the different elements of data governance (ranging from data strategies and institutional and regulatory frameworks to infrastructure and architecture) are nested within public sector digital transformation efforts, and/or digital government policies. However, while policy and decision makers within line and co-ordination ministries (e.g. environment, transport, finance, public administration) increasingly recognise the relevance of "data as an asset" in their policy discourse (see Chapter 3), these policies often ignore the key contribution of data governance to policy success. This context is not endemic to the public sector, for "today there is wide agreement that data is a critical asset [*among businesses*], but that doesn't always translate into taking the necessary actions to make that asset deliver real advantages" (Algmin and Zaino, 2018[14]).

This particularly relevant in the context of cross-cutting public policies that require the sharing of, and access to, data from multiple public sector organisations for policy monitoring, compliance and evaluation purposes (e.g. public sector integrity, public budgeting, regulatory policy), or in the context of cross-sectoral data-sharing practices and governance arrangements (e.g. business-to-government data sharing) (see Flexibility and scalability later in this chapter).

Public policies other than digital government can benefit from data governance as an underlying, yet mission-critical, element for policy success. When feasible, this could be achieved by embedding different data governance elements in existent organisational and policy structures. By doing so, policy makers can enable the right context and move from the overused discourse on data as an asset to the definition of an environment where data serve specific needs across the whole policy cycle.

> *e) Good data governance does not happen in isolation. It benefits from the adoption of open, inclusive, iterative, collective and value-based approaches to its definition, implementation, evaluation and change.*

Good data governance is not the responsibility of a small group of people. It should reflect the needs of a globalised, fast-paced, diverse, digitalised and inter-connected world. Public sectors need to move away from closed and isolated ways of defining, implementing, monitoring and evaluating their data governance frameworks and tools.

Governments can benefit from adopting open, inclusive, iterative, collective and value-based data approaches when putting in place their data governance initiatives. For instance, stakeholder engagement can help to better identify data policy priorities and data needs, and to assess the current context in terms of data capability within the public sector. Iterative engagement can also help to identify changing trends in order to take action and modify the rules and tools supporting data governance.

In addition, establishing partnerships with actors outside the public sector can help to:

- take advantage of private sector digital solutions to improve, streamline and modernise the public sector data infrastructure (e.g. cloud or Software-as-a-Service solutions)
- promote the publication of data produced by civil society organisations on government open data platforms or the publication of open government data on non-governmental data portals[3]

- support data sharing among multiple stakeholders from different sectors and increase data owners' control and decision power over the sharing and use of their data to address common policy challenges[4] (e.g. see Box 2.1. Deploying data trusts as tools in the pursuit of common value).

Good data governance also benefits from establishing a system of shared values and skills where all actors of the data ecosystem support and are responsible for policy success (e.g. data stewardship is shared among all relevant actors). At the same time, it implies defining and deploying a set of open and shared tools (e.g. open standards, APIs and algorithms) that can help in promoting integration within and outside the public sector.

Box 2.1. Deploying data trusts as tools in the pursuit of common value

In the process of accelerating the collection and sharing of data to harness artificial intelligence and other emerging technologies, governments, businesses and other organisations face the increasing need of exploring and deploying sound tools for the management of data to protect the rights of data owners while addressing common goals. Governments are therefore starting to explore new instruments that can facilitate ethical and fair data sharing between different actors of the data ecosystem.

For instance, as part of the OECD project on enhancing access to and sharing of data, partnerships such as "community-based data-sharing agreements" have been discussed as ways of increasing access to data while ensuring it is done safely and ethically ***(OECD, 2017[15]).*** These types of partnerships or frameworks highlight the flexible and forward-looking approach of data governance in managing potential risks from data sharing.

Data trusts add to the above-mentioned proposed data governance tools. They build on long-standing legal trust frameworks applied to the management of data, and can be used to promote data sharing in areas where it is not currently happening. As defined by the (Open Data Institute, 2018[16]), a data trust is a "legal structure that provides independent stewardship of data". Independent trustees are liable to take decisions about the data in accordance with the interests of the trust's beneficiaries, who may be other organisations, citizens, end consumers or data users, by upholding laws and abiding by rules made when the data trust was set up. As described by (Wylie and McDonald, 2018[17]), it helps to view data trusts as containers that holds assets, define governance and manage liabilities. The terms ruling data trusts can be adjusted depending on the data type or actors involved. Thus, this flexibility can support the adoption of "anticipatory regulation", a new regulatory framework developed by Nesta,1 in the context of data governance (Element AI and Nesta, 2019[18]).

In 2018, the United Kingdom launched its AI Sector Deal, a GBP 0.95 billion support package from government and industry to keep the United Kingdom at the forefront of the artificial intelligence and data revolution (BEIS and DCMS, 2018[19]). As part of the deal, the government committed to explore data-sharing frameworks such as data trusts together with the artificial intelligence industry. The UK government partnered with the Open Data Institute (ODI) to explore how a data trust, as defined by the ODI, could increase access to data while retaining trust. As part of this work, the ODI worked with three pilot projects focused on diverse challenges: tackling illegal wildlife trade, reducing food waste and improving public services in Greenwich. The findings and recommendations of these pilots were published in April 2019 (Office for Artificial Intelligence, 2019[20]).

Note: For more information see: https://www.nesta.org.uk/report/renewing-regulation-anticipatory-regulation-in-an-age-of-disruption.
Sources: OECD with contributions from the UK Office for Artificial Intelligence and NESTA; Element AI and Nesta (2019[18]), Data Trusts: A New Tool for Data Governance, https://hello.elementai.com/rs/024-OAQ-547/images/Data_Trusts_EN_201914.pdf; BEIS and DCMS (2018[19]), AI Sector Deal, https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal; Wylie, B. and S. McDonald (2018[17]), What Is a Data Trust?, https://www.cigionline.org/articles/what-data-trust; OECD (2017[15]), Programme for OECD Expert Workshop – Enhanced Access to Data: Reconsiling Risks And Benefits of Data Reuse, https://www.oecd.org/internet/ieconomy/oecd-expert-workshop-enhanced-access-to-data-copenhagen-programme.pdf; Open Data Institute (2018[16]), "Defining a 'data trust'", https://theodi.org/article/defining-a-data-trust; Office for Artificial Intelligence (2019[20]), AI Sector Deal One Year On, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819331/AI_Sector_Deal_One_Year_On__Web_.pdf.

Developing a common framework for public sector data governance

While some countries have made advancements in clearly defining public sector data governance models, others have opted for a less strict approach where data governance is not explicitly acknowledged, but takes place in an implicit fashion.

For instance, **Luxembourg** is working towards the development of a data governance framework in the context of the recently adopted National Interoperability Framework. This work aims at taking a more progressive approach that adopts the three core principles of digital first, once-only and transparency in the context of public sector data efforts. Luxembourg's National Interoperability Framework also sets objectives to promote open data, open standards and interoperability, machine-readable and linked data, APIs and open source software in the public sector.

Yet, approaches to public sector data governance may vary in terms of focus (e.g. a focus on technical governance aspects) or reach (e.g. specific data governance elements are available but dispersed).

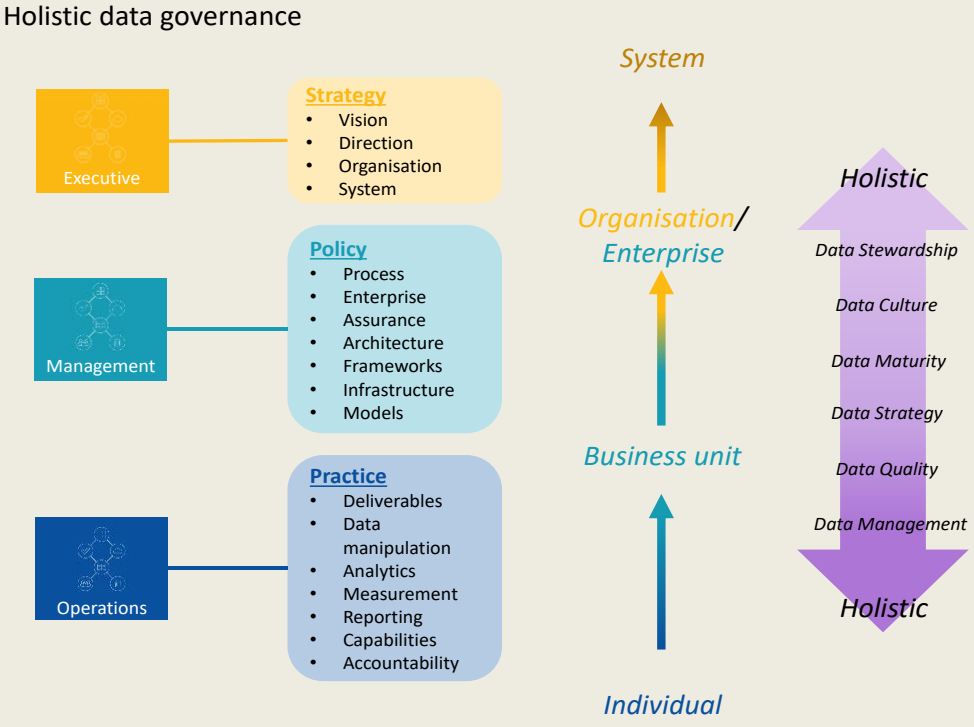
For this reason, the OECD proposes a holistic model for data governance in the public sector as an effort to bring greater clarity and structure to the definition and implementation of the concept across countries. The model is based on the extensive OECD work on digital government and government data and additional research carried out by the OECD Secretariat. Earlier versions of the model can be found in previous OECD digital government reviews, namely the *OECD Digital Government Review of Norway* (OECD, 2017[21]), the *OECD Digital Government Review of Sweden* (OECD, 2019[22]), the *OECD Digital Government Review of Peru* (OECD, 2019[23]) and the *OECD Digital Government Review of Argentina* (OECD, 2019[3]).

Box 2.2. Data governance frameworks in the public sector: Examples from OECD countries

New Zealand

The leading agency for government-held data in New Zealand (Stats NZ) developed a new and improved data governance framework for the New Zealand government. The framework is part of the agency's numerous efforts to promote better data management practices across the public sector, and to leverage data as a strategic asset for decision making. One of the central pillars of the framework is the adoption of a so-called "whole-of-data life cycle approach", meaning public bodies and employees are encouraged to think more strategically about the governance, management, quality and accountability of their data, over the whole data life cycle (i.e. from the design and source of the data to its storing, publication and disposal).

Figure 2.1. New Zealand: Data governance framework

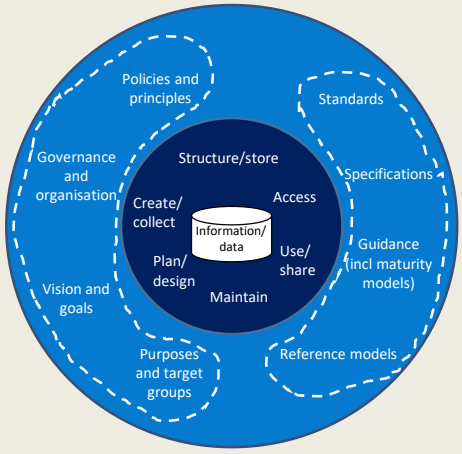


Source: Sweeney, K. (2019[24]), *"An operational data governance framework for New Zealand government"*, https://statsnz.contentdm.oclc.org/digital/collection/p20045coll1/id/2657.

Norway

As part of its work in developing Norway's national IT architecture, the Agency for Public Management and eGovernment created an information governance model that positioned the management of public sector data at the centre of the digital transformation of the Norwegian public sector. By placing data at the heart of the information governance model, and by complementing it with strategic visions, policies, principles, standards and guidelines for better use of public sector data, public bodies in Norway have been given a rich set of tools to help leverage data as a strategic asset for decision making and reuse.

Figure 2.2. Norway: Information governance model



Source: OECD (2017[21]), *Digital Government Review of Norway: Boosting the Digital Transformation of the Public Sector,* https://doi.org/10.1787/9789264279742-en.

Estonia

The data governance framework in Estonia is built on three core components – data source, handling and storage, and purpose – and stresses the importance of identifying and linking different data sources (e.g. private sector data, administrative data and census data) to different types of data usages (e.g. policy analysis, research, operational), in order to strategically ensure the proper handling and storage of data.

Four main challenges (the gathering, guarding, growing and giving of data) are identified as crucial to face in order to create a better data governance framework. These challenges cover a large section of the data value chain, from understanding data assets and establishing data governance principles to data processing, data sharing and dissemination of meta information.

Source: Sweeney, K. (2019[24]), "An operational data governance framework for New Zealand government", https://statsnz.contentdm.oclc.org/digital/collection/p20045coll1/id/2657; (2017[21]), Digital Government Review of Norway: Boosting the Digital Transformation of the Public Sector, https://doi.org/10.1787/9789264279742-en; Mägi, M. (2019[25]), "Data for law making".

Good data governance promotes integration and systemic coherence, and offers a common basis to use data in order to attain shared policy goals and promote trust. Ergo, the model intends to highlight the value of all organisational, policy and technical aspects for successful data governance. It identifies a range of (non-exclusive) data governance elements and tools, and organises them into six different groups. (a-f; see Figure 2.3. Data governance in the public sector)

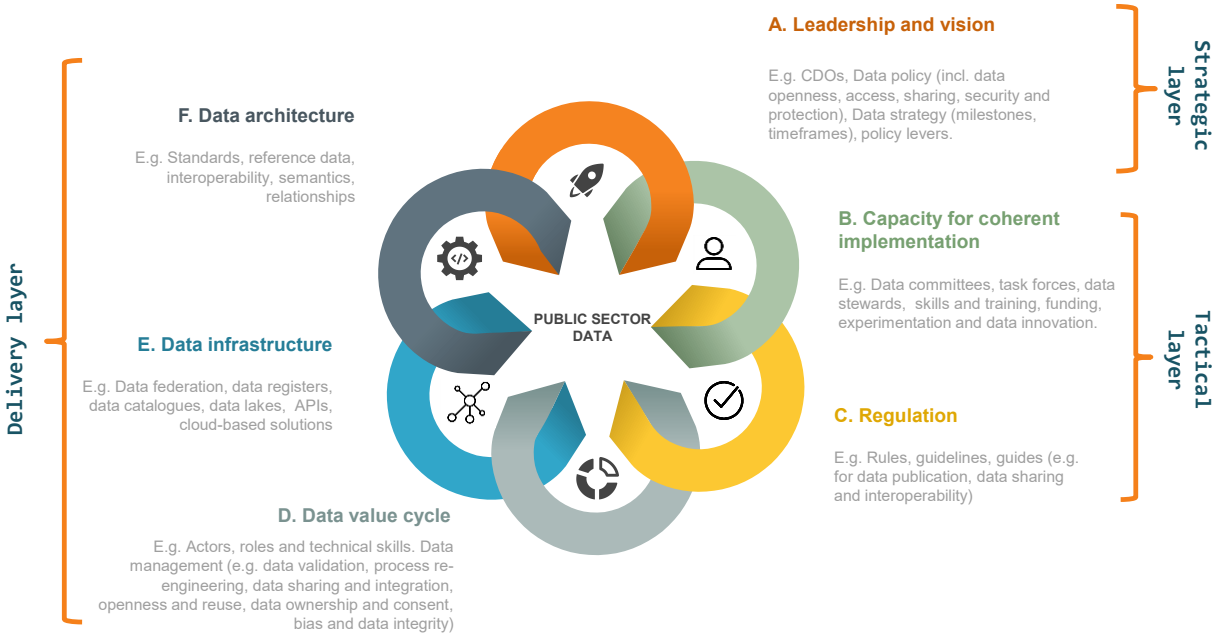
These six groups are then arranged under three core layers of data governance (strategic, tactical and delivery) using the three traditional data governance categories as guidance (strategic, tactical and operational) as discussed and/or presented in Ghavami (2015[5]), DAMA Internal (2017[26]) and the BARC's 9-Feld-Matrix [see Grosser (2013[27]) and BARC (2019[28])]. The model is also based on additional research, including Ladley (2012[29]) and Sen (2019[30]):

- **Strategic layer [including (a) Leadership and vision]**: Some of the data governance elements in this layer include national data strategies and leadership roles. It is worth noting that the model considers data strategies as an element of good data governance. This argument rests on the fact that data strategies enable accountability and can help define leadership, expectations, roles and goals. The strategic layer also highlights how the formulation of data policies and/or strategies can

benefit from open and participatory processes, thus integrating the inputs of actors from within and outside the public sector towards greater policy ownership.

- **Tactical layer [including (b) Capacities for coherent implementation and (c) Legal and regulatory frameworks]**. It enables the coherent implementation and steering of data-driven policies, strategies and/or initiatives. It draws upon the value of public sector skills and competences, job profiles, communication, co-ordination, and collaboration as instruments to improve the capacity of the public sector to extract value from data assets. It also highlights the value of formal and informal institutional networks and communities of practice as levers of public sector maturity and collective knowledge. This layer also comprises data-related legislation and regulations as instruments that help countries define, drive and ensure compliance with the rules and policies guiding data management, including data openness, protection and sharing.
- **Delivery layer [including (d) Integration of the data value cycle, (e) Data infrastructure and (f) Data architecture]**. The delivery layer allows for the day-to-day implementation (or deployment) of organisational, sectoral, national or cross-border data strategies. It touches on different technical and policy aspects of the data value cycle across its different stages (from data production and openness to reuse), the role and interaction of different actors in each stage (e.g. as data providers), and the inter-connection of data flows across stages. Each stage is inter-connected but has specific policy implications in relation to the expected outcomes. For instance, data-sharing initiatives (e.g. the production of good-quality, standardised and interoperable government data) can contribute to data reuse by external actors in later stages (e.g. as open government data). The adoption of technological solutions (e.g. cloud-based data-hosting services, APIs, data lakes) takes place in this layer for it supports those policy goals defined in the strategic layer. It also relates, for instance, to the need for re-engineering legacy data management practices and processes or retrofitting and adapting legacy data infrastructures. Data interoperability and standardisation also take place at this level.

Figure 2.3. Data governance in the public sector



Source: OECD (2019[3]), *Digital Government Review of Argentina: Accelerating the Digitalisation of the Public Sector*, https://doi.org/10.1787/354732cc-en.

The elements used to exemplify the plethora of policy instruments, arrangements, initiatives and/or tools that can be used by countries to deploy their data governance frameworks is not exhaustive. Thus, countries might opt for adopting different data governance elements and tools that better fit their national context and public sector culture in line with the proposed three layers and the six underlying categories presented in the model.

For the purpose of the analysis presented in this chapter, the data governance model explores practices at the national level (e.g. national data strategies, central data standards and national data-sharing platforms).

Flexibility and scalability

The proliferation of data governance frameworks and tools in the public sector can hinder the integration of data and processes. Common policy goals (e.g. data protection) require coherent data governance frameworks, meaningful instruments (e.g. policies, regulations) and shared tools (e.g. data infrastructures, standards) that can help advance the cohesive deployment of data efforts in the public sector. Yet, the definition of a common data governance framework (from regulations and policy levers to standards and data federation tools and standards) should also allow for flexibility and scalability in order to avoid fragmentation; promote integration; and increase the adoption of good governance practices across organisations, levels of government, policy areas, sectors and borders.

This balance between adopting a structured approach and allowing for flexibility and scalability can help foster a common understanding, alignment and coherence of data efforts to support concerted actions and address shared policy challenges and deliver joint policy results. Additionally, it can help to adjust the data governance model and its tools to specific contexts, and respond to changing needs (e.g. anticipatory regulation) or ad hoc policy needs (e.g. different policy areas and stakeholders).

These arguments lay on the government as a platform dimension of digital governments (see Chapter 1). Thus, the development of a coherent data governance framework enables the deployment and adoption of common data solutions and tools among public sector organisations.

The different elements presented in the model and in this chapter address data governance from a national perspective (see the Overview of public sector data governance practices later in this chapter). However, the model is relevant in different contexts (inter-institutional, cross-border) where public sector data governance plays a key role in terms of enabling the sharing of and access to data.

The nature of the actors involved (the data ecosystem) can add to the complexity of the data governance environment as different actors have different needs and characteristics (e.g. sector, size) as well as differing digital and data maturities. However, the need for greater structure, flexibility, control, enforcement and compliance will also increase as the complexity of the data governance environment evolves; its purpose matures; the needs of actors change; and depending on whether it is implemented in a decentralised, federated or multinational context.

Organisational

At this level, data are shared across units or departments and bodies within the same public sector organisation. Thereby, data governance can improve the management, sharing of and access to data only within organisational boundaries. The need for a common data governance framework and shared data governance tools increases once actors external to the organisation join the data ecosystem.

Sector- or policy-specific

Good data governance can also benefit a pool of public sector organisations that share common goals and mandate, and produce, need to access, share or reuse common datasets.

Earlier OECD efforts to promote good data governance in specific policy areas include the OECD *Recommendation of the Council on Health Data Governance*. It provides a set of principles to "encourage greater availability and processing of health data within countries and across borders for health-related public policy objectives, while ensuring that risks to privacy and security are minimised and appropriately managed" (OECD, 2017[31]).

Examples of data governance initiatives in specific policy areas include the Geodata Strategy of the National Land Survey Authority in **Sweden**. The Geodata Strategy brought greater coherence, and defined a set of common goals to foster the value of geodata for efficiency, innovation, competitiveness and the achievement of Agenda 2030 (Lantmäteriet, 2016[32]). The four pillars of the Swedish Geodata Strategy address different data governance elements, including interoperability, standardisation, openness and user engagement (OECD, 2019[22]).

The **United Kingdom's** Ordnance Survey provides another example of a maturing and more strategic sectoral data governance environment. In 2017, the Ordnance Survey (the UK national mapping authority) named its first chief data officer (Ordnance Survey, 2017[33]) and in 2019 it released its data strategy in order to continue delivering the benefits of sharing and opening accurate and quality mapping data for business impact (CIO UK, 2019[34]).

The Swedish and UK cases provide an organised and solid approach to opening up government data and highlight how the sharing of good-quality and trustworthy data requires taking action in the earlier stages of the data value cycle (e.g. data production) (see the Overview of public sector data governance practices later in this chapter).

Another application case is that of the evidenced-based policy-making work carried out by the Japanese government. **Japan** has defined and implemented a strong evidenced-based and data-driven approach to improve the impact of policies and public services since 2017. This work draws upon data governance regulatory instruments published by the Japanese government, namely the Basic Act on the Advancement of Public and Private Sector Data Utilisation. For this purpose, the central government established a governance structure to ensure the coherent implementation of evidenced-based policy-making approaches across the broad public sector, including the establishment of a cross-ministerial council (which also benefits from the advice of external advisors), and the appointment of a director-general for evidenced-based policy making across all ministries at the central level. This case highlights the benefits of data governance and data itself for policy monitoring and effective decision making in the public sector (Fukaya, 2019[35]).

In **Argentina**, the Ministry of Justice developed a tool to improve the sharing of personal data in the context of judicial investigations using the central common interoperability platform (INTEROPER.AR). The tool allows registered users (e.g. tribunals, prosecutors, courtrooms) to request data from and between those data registers connected to the interoperability platform (OECD, 2019[3]), therefore speeding up data access and reducing the time to respond to citizens.

While in Argentina there is a need for formalising data governance structures at the strategic layer, this case illustrates the potential scalability of the interoperability tool. For instance, its application can be expanded to other policy areas, including public sector integrity, as recommended in the OECD *Digital Government Review of Argentina* (OECD, 2019[3]) and the OECD *Integrity Review of Argentina* (OECD, 2019[36]). However, such an approach would require reinforcing the underlying data governance arrangements for public sector integrity while developing, implementing and/or adapting the specific rules and tools in order to respond to the ad hoc requirements of integrity policies.

This is particularly relevant as public sector integrity is a complex topic covering different areas with actors sharing and requesting common data taxonomies for monitoring, reporting and/or auditing purposes (e.g. declarations of interest, gifts, open contracting data, beneficial ownership, budget data). Therefore, the importance of establishing a solid data architecture and infrastructure (technical layer) does not rest exclusively on its benefits to inter-institutional data sharing, but on the value of streamlined data-sharing practices as a means to identify relationships between different stakeholders and reduce, monitor, control or address integrity risks.

Multilevel

Another level of complexity is added when data sharing takes place in a multilevel governance context. For instance, in federal models of government, the balance between central and local power has an impact on how the central government can access specific datasets owned and produced by local authorities.

In **Mexico**, a federal country, the central government developed the Open Mexico Network (*Red Mexico Abierto, 2015-2017*) to engage local governments in the central open data policy, and facilitate the publication of open government data produced by local authorities on the central open data portal datos.gob.mx. For this purpose, the central government created a network of institutional contact points within public sector organisations at the state and municipality levels. This institutional fabric improved communication and co-ordination, but it also "ensured the efficient flow of tools and support provided by the federal government for the standardisation and publication of open government data" (OECD, 2018[37]).

Also, while central authorities can define overarching data quality standards, in practice the responsibility for data quality falls on local governments, increasing the need for developing the right controls to ensure that data are produced in line with central standards for policy monitoring purposes.

In **Thailand**, the former Ministry of Information Communication Technologies (now the Ministry of Digital Economy) designed a multilevel mechanism for reporting development data across all levels of government. While this initiative did not move forward, its architecture implied a complex data collection and sharing model, thus involving authorities at the local, provincial, departmental and ministerial levels, under the leadership of the Office of the Prime Minister (OECD, forthcoming[38]). This blend of actors, roles and responsibilities requires strict data quality controls to ensure the quality, integrity and trustworthiness of the data across the whole data value cycle. Indeed, most of these authorities still face legacy challenges resulting from data fragmentation, duplicate standards, legal barriers and slow data-sharing processes, thus hampering the timely access to data for policy and decision making (Wuttisorn, 2019[39]) and reinforcing the need for a solid data governance.

Cross-sector

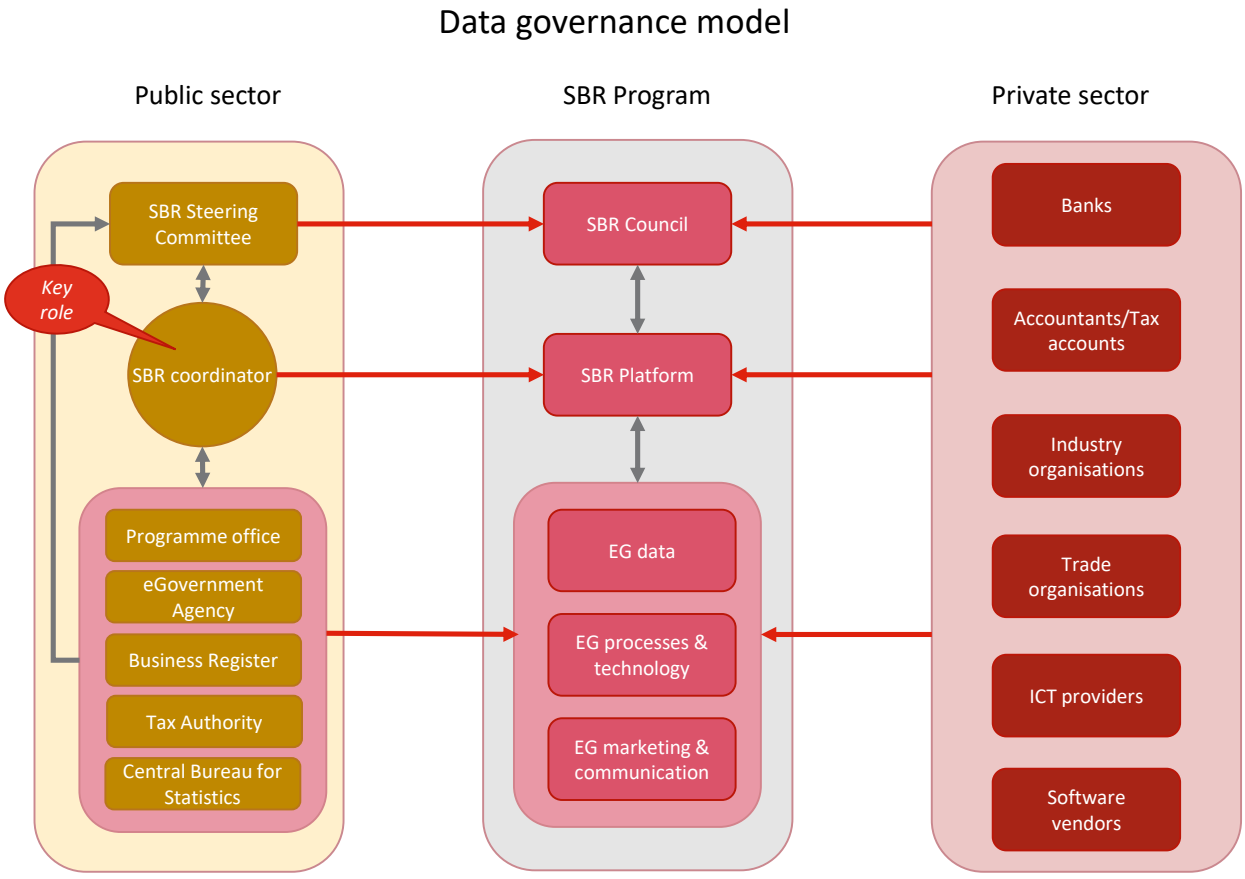
Common data governance frameworks contribute to the effective implementation of cross-sector data collection, sharing and/or accessing initiatives. For instance, in the context of regulatory compliance, business-to-government reporting practices can benefit from the implementation of common data governance structures and tools across all layers of the governance model.

In the **Netherlands**, the Standard Business Reporting (SBR)[5] reduced the burden imposed on businesses in the provision of business information to local authorities and banks (SBR, 2019[40]). For this purpose, the SBR defined a shared public-private data governance framework creating, among others:

- A Steering Committee within the public sector in charge of defining the SBR's goals and programme of work, and a council in charge of deciding the course of action, which benefits from insights from public and private sector actors. These elements reinforce the SBR's data governance strategic layer.

- At the tactical layer, the SBR created a co-ordinator role to ensure coherent implementation of the programme. The SBR also created a devoted platform where public and private sector actors can monitor and provide advice on the implementation of the programme.
- At the delivery layer, the SBR standardised data definitions using a common data taxonomy defined by the Dutch government, and streamlined and defined common reporting processes. The digital government service (Logius)[6] of the Dutch Ministry of the Interior and Kingdom Relations provides support on the technical aspects of the SBR.

Figure 2.4. Netherlands: Standard Business Reporting



Source: Groenveld, B. (2019[41]), Standard Business Reporting (SBR).

Cross-border

Increased data flows across borders demand greater government action to ensure the protection and ethical use of data, particularly citizens' data, when those are collected, processed and used by organisations from all sectors. The policy implications of cross-border data flows, both in terms of positive and negative benefits, are thus vast, and policy success requires the involvement of a plethora of actors at the global scale, from international organisations to businesses, data protection authorities and civil society organisations. OECD instruments such as the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD, 2013[42]) have sought to bring greater coherence to cross-border data protection policies and initiatives across OECD member and partner countries.

Transborder data flows have specific implications for public governance and call for stronger international data governance arrangements and coherent multinational action.

Reinforcing cross-border data governance can help to better monitor transnational infrastructure projects and propel greater regional integration (for example the Australia & New Zealand Infrastructure Pipeline, ANZIP)[7]. It also can support joint policy actions of governments to prevent, combat and tackle corruption at the regional level (e.g. by harmonising and enabling shared regulatory frameworks to allow data-driven evidence to be used for auditing purposes within and across governments, facilitating data access and sharing, etc.).

Shared data governance frameworks can also help to improve cross-border public service delivery. For instance, in 2013 **Estonia and Finland** agreed on a common agenda for the development of digital government as means to support the implementation cross-border digital services in areas such as tax, health and education (OECD, 2015[43]). This enabled the deployment of Estonia's X-Road data-sharing platform[8] (see the Overview of public sector data governance practices later in this chapter) in Finland. The inter-connection of both Estonia's and Finland's X-Road platforms in 2018 (VRK, 2018[44]) has also led to greater, automated and secured cross-border data sharing, benefiting service users and supporting the future development of additional cross-border services in the region.

The success of the cross-border deployment of the X-Road between Estonia and Finland not only relies on technical issues; it also highlights the value of shared data governance policy structures at the strategic level. Drawing on the bilateral agreement signed in 2013, in 2017 Estonia and Finland agreed on the creation of the Nordic Institute for Interoperability and Solutions, which "ensure(s) the development and strategic management of the X-Road and other cross-border components for eGovernment infrastructure" (NIIS, 2019[45]).

Overview of public sector data governance practices at the national level across OECD member and partner countries

This section presents a brief overview of national practices across OECD member and partner countries. When feasible, it presents evidence and data collected through different activities across the OECD under digital government. These include national peer reviews, cross-national reports, OECD surveys on digital government and open data, the work on data-driven public sector.[9]

Strategic layer

National data strategies

The importance of better managing, protecting and sharing data within the public sector is gaining traction across the OECD. In front-runner countries, this has led or is leading to the development of holistic national data strategies. These strategies are often nested within public sector digitalisation efforts. Notable examples include the **United States'** Federal Data Strategy, **Canada**'s Data Strategy Roadmap for the Federal Public Service, the Government Data Agenda in the **Netherlands** and **Ireland's** Public Service Data Strategy.

For instance, the **Dutch Government Data Agenda** centres on the value of data as a tool to address policy and social challenges. The Dutch Ministry of the Interior and Kingdom Relations leads the implementation of the agenda, but both central and local governments are responsible for implementing it.

The agenda also "pays specific attention to the protection of public values and fundamental rights" (BZK, 2019[46]), thus including policy issues related to data ethics and the algorithm transparency. The agenda integrates policy goals oriented to better data management in the public sector and the publication and reuse of open government data. The relevance of the public sector's organisational culture and knowledge-sharing for transformation change are also underlined, which is in line with the OECD approach for the digital transformation of the public sector [see, for instance, OECD (2019[22])].

In **Ireland**, the central government recently launched the Public Service Data Strategy for 2019-2023.[10] The Irish data strategy draws upon earlier data initiatives and policy instruments, including the National Data Infrastructure and the Open Data Strategy. The Irish data strategy is clear on the need for bringing a unified approach to public sector data initiatives and defining shared principles, goals and actions in order to support public sector cohesion (Office of the Government Chief Information Officer, 2019[47]).

Box 2.3. The United States: 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. The data strategy centres on three core principles (ethical governance, conscious design and a learning culture). It adds to several existing initiatives, policies, executive orders and laws that over the past few decades have helped make the United States a front-runner in terms of strategic management and reuse of government data.

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 its early phase, federal agencies are required to adhere to annual government action plans that include prioritised steps, time frames and responsible entities. A draft version of the 2019-2020 Federal Data Strategy Action Plan covers 16 steps seen as critical to launch the first phase of the data strategy vision, including the development of data ethics frameworks and data science training for federal employees.

Sources: Executive Office of the President (2019[48], Federal Data Strategy: A Framework for Consistency, https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-18.pdf; Federal Data Strategy Development Team (2019[48])), 2019-2020 Draft Federal Data Strategy Action Plan, https://strategy.data.gov/action-plan.

The design process of national data strategies is also relevant. The OECD has observed, for instance, that late stakeholder engagement in the development of public sector digitalisation strategies can decrease policy awareness, clarity, accountability and ownership [see, for instance, OECD (2019[22])]. Early engagement can help identify policy challenges that would otherwise be ignored, and bring relevant actors on board prior to the implementation of these strategies.

One relevant example in this respect is the open consultation process launched by the Department for Digital, Culture, Media and Sports in the **United Kingdom** for the development of the UK National Data Strategy. In June 2019, the Department for Digital, Culture, Media and Sports carried out a public consultation to collect evidence and inform the development of its National Data Strategy.[11] The development of the data strategy will be followed by a series of roundtables and testing exercises towards the publication of the final document in 2020 (DCMS, 2019[49]).

It is also important to mention that while countries are moving towards holistic policy approaches for public sector data practices, a vast group of OECD member and partner countries have had more focalised data policies for some time. Examples worth mentioning are the open data policies in countries like **France**, **Korea** and **Mexico** (OECD, 2018[6]), and well-grounded data register policies in **Denmark, Italy, Norway** and **Sweden**.

The Danish Basic Data Registers programme,[12] which dates back to 2013, has evolved from a strong focus on data-sharing practices within the public sector to a hybrid approach where core public sector data assets are shared for public access and reuse through a public data distributor.[13] In addition, the programme puts an emphasis on integration, for it allows for public sector data access through web services and APIs (OECD, 2018[50]).

Leadership

The institutional governance model is also a core element of good data governance, as it provides clarity in terms of leadership and accountability. It is, however, important to make a distinction between political and administrative leadership roles. On the one hand, political leadership provides the high-level support needed to advance the policy agenda; however, changes of political administration can lead to vacant positions, resulting in reduced political support for data policies.[14] On the other hand, the leadership of top management positions helps to implement and steer policy design and implementation, thereby increasing the continuity and sustainability needed to deliver results across political terms.

That said, some countries have formalised leadership roles by attaching them to existent administrative structures. Relevant examples include the Government Chief Data Steward in **New Zealand,** which is held by the Chief Executive of Statistics New Zealand. The Government Chief Data Steward is in charge of leading the data policy in the country.[15] New Zealand's case is also relevant in terms of policy accountability, as Stats NZ releases a quarterly dashboard "highlighting key deliverables for their data leadership role" under the Government Chief Data Steward (Stats NZ, 2019[51]).

An earlier example is that of **France**'s *Administrateur Général des Données*, created in 2014 (French Government, 2014[52]) and attached to the responsibilities of the head of the Etalab[16] (the task force within the Office of the Prime Minister in charge of co-ordinating the open data and artificial intellignece policy in France). In **Canada**, the Data Strategy Roadmap for the Federal Public Service recommends the creation of a Government Chief Data Steward as a means to "clarify roles and responsibilities around enterprise data leadership" (Government of Canada, 2018[53]).

Others, however, have followed different leadership models, which are less hierarchical and shared by different individuals, and respond more to the culture within their public sector. This scenario is observed, for instance, in Nordic countries like **Sweden**, where the central government has opted for a more consensus-based leadership model in the form of a data taskforce composed of leading public sector agencies (OECD, 2019[22]).

In either scenario, the need for a clear leadership is a precondition to help to achieve policy goals (OECD, 2019[3]). It is also worth mentioning that in some cases, open data leadership positions might act as chief data officer (CDO) *de facto*, as in the case of **Argentina** (OECD, 2019[3]) and **Mexico** (OECD, 2016[54]).

Tactical layer

Good data governance enables the coherent implementation of data policies. Yet, successful policy implementation relies on the intersection of different factors, ranging from the establishment of inter-institutional co-ordination bodies grounded in adequate institutional networks to capacity-building initiatives, collaboration and knowledge-sharing. Also, while complex, the availability of the appropriate regulatory frameworks (e.g. for data sharing, openness and protection) helps to create the right environment for policy instrumentation (e.g. by reducing burdens and barriers to data sharing), and in setting the rules for better controlling data management practices in the public sector.

Steering and policy co-ordination bodies

Examples of policy steering or co-ordination bodies include, for instance, **Ireland**'s Data Governance Board, which was created to formalise a sustainable "governance structure for the Public Service, through which the development and implementation of data management standards, guidelines and activities can be overseen" (Office of the Government Chief Information Officer, 2019[47]).

In the **United States**, the draft action plan of the Federal Data Strategy foresees the creation of a Data Council within the White House Office of Management and Budget (OMB) by November 2019 (Federal Data Strategy Development Team, 2019[48]). While the OMB Data Council will help in co-ordinating the

Federal Data Strategy, it will also have the role of informing OMB's "budget priorities for data management and use" (*idem*). These bodies can also play an important advisory role in ensuring that data strategies take a risk-management approach, and anticipate and respond to policy challenges as they emerge. The Data Ethics Advisory Group in **New Zealand** (see Chapter 4) provides an example in this regard.

Chief data officers, institutional networks and data stewardship

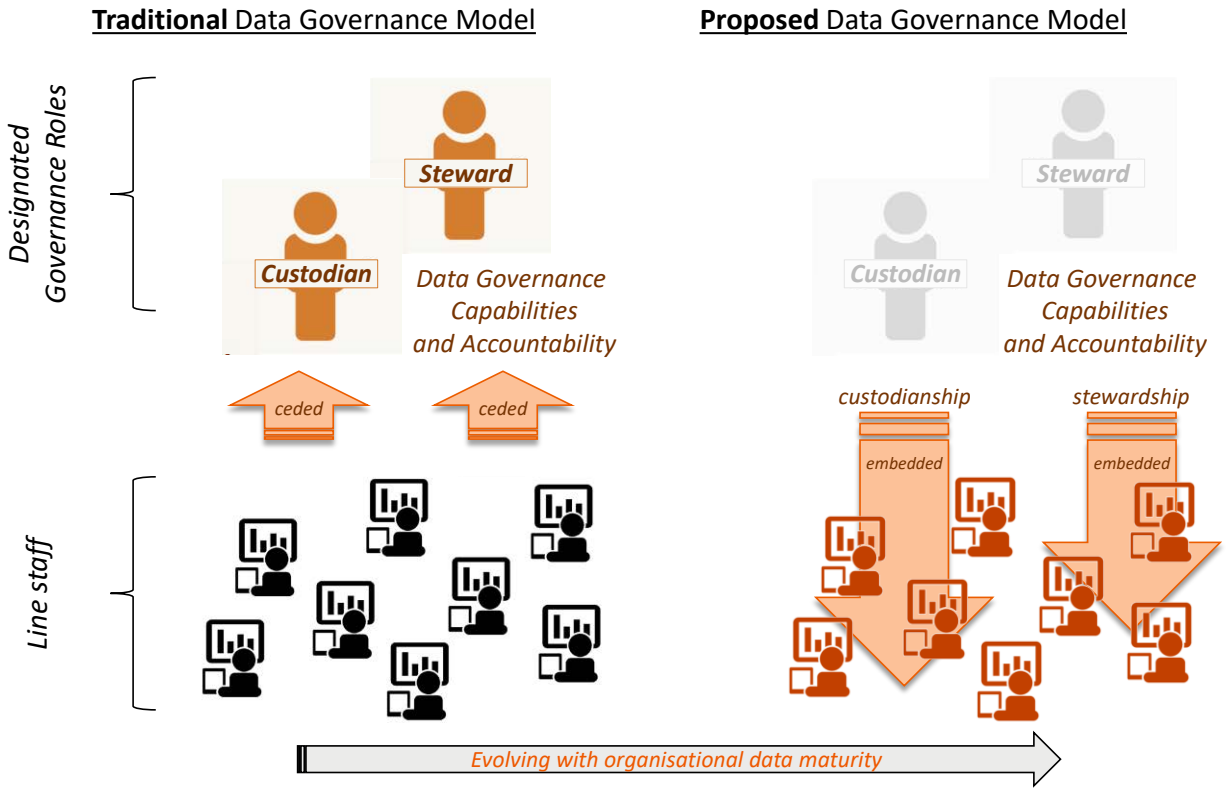
The need for stronger institutional networks and data stewardship in the public sector is also a growing priority for countries. This draws upon the urgency to enact a paradigm shift from a primarily technical perspective to one focused not only on compliance and control over data management and sharing practices, but also on strategic goals and fostering a problem-solving approach, centred on citizens.

As illustrated in previous OECD work on digital government and open data [see (OECD, 2016[55]; 2018[6]; 2019[56])], some countries have made a clear distinction between technical and strategic data roles in the context of open data policies as a means to emphasise that digital and data-driven transformation goes beyond mere technical aspects.

For instance, in **Korea**, the 2013 Act on the Promotion, Provision and Use of Public Data established the roles of "officers responsible for the provision of public data" and "data manager". Officers responsible for the provision of public data are in charge of co-ordinating the central open data policy at the organisational level, translating its goals into clear actions and liaising with other organisations for this purpose. Data managers are in charge of administrative and technical tasks, including compliance with data standards, data quality and data publication.

In the context of national data strategies, **New Zealand**'s operational Data Governance Framework[17] provides an interesting example where data stewardship is seen more as a skill to be built up among public officials rather than a formal role. This approach aims to embed "*data accountability and best practice data management across all data-handling positions, with the goal of evolving beyond the need for traditional data governance roles (e.g. data custodians, data stewards)*" (Sweeney, 2019[24]).

Figure 2.5. New Zealand: Data stewardship in the public sector (proposed model)



Source: Sweeney, K. (2019[24]), *"An operational data governance framework for New Zealand government"*, https://statsnz.contentdm.oclc.org/digital/collection/p20045coll1/id/2657.

In the **United States**, the 2018 Foundations for Evidence Based Policymaking Act (signed into law on 14 January 2019) directs the head of each agency to "designate a non-political appointee employee in the agency as the chief data officer of the agency" (US Congress, 2019[57]). This is part of the provisions of the Open, Public, Electronic, and Necessary Government Data Act (OPEN Government Data Act), which is one component of the Evidence-Based Policymaking Act (OECD, 2019[3]). These efforts contribute to building a more mature data governance ecosystem within the public sector, which can help to address potential sustainability risks across political administrations.

Box 2.4. United States: Chief data officers

The provisions of the Open, Public, Electronic, and Necessary Government Data Act describe the activities and role of institutional chief data officers as follows:

The chief data officer of an agency shall:

1. be responsible for life cycle data management
2. co-ordinate with any official in the agency responsible for using, protecting, disseminating and generating data to ensure that the data needs of the agency are met
3. manage data assets of the agency, including the standardization of data format, sharing of data assets and publication of data assets in accordance with applicable law
4. (…)
5. (…)
6. ensure that, to the extent practicable, agency data conform with data management best practices
7. engage agency employees, the public and contractors in using public data assets and encourage collaborative approaches on improving data use
8. support the performance improvement officer of the agency in identifying and using data to carry out the functions described in Section 1124(a)(2) of Title 31
9. support the evaluation officer of the agency in obtaining data to carry out the functions described in Section 313(d) of Title 5
10. review the impact of the infrastructure of the agency on data asset accessibility and co-ordinate with the chief information officer of the agency to improve such infrastructure to reduce barriers that inhibit data asset accessibility
11. ensure that, to the extent practicable, the agency maximizes the use of data in the agency, including for the production of evidence (as defined in Section 3561), cybersecurity and the improvement of agency operations
12. identify points of contact for roles and responsibilities related to open data use and implementation (as required by the director)
13. serve as the agency liaison to other agencies and the Office of Management and Budget on the best way to use existing agency data for statistical purposes (as defined in Section 3561)
14. comply with any regulation and guidance issued under Subchapter III, including the acquisition and maintenance of any required certification and training.

Source: US Congress s (2019[57]), H.R.4174: Foundations for Evidence-Based Policymaking Act of 2018, https://www.congress.gov/bill/115th-congress/house-bill/4174/text.

Legal and regulatory frameworks

Regulation plays a key role in the context of data governance, thus its implications in this respect are vast. Regulation helps in defining the set of rules to control the access to and sharing of data, promote openness, and ensure and enforce the protection of sensitive data. These instruments help also in the definition and enforcement of common data standards towards greater data interoperability and streamlined data-sharing practices. However, regulation can also be an obstacle for good data governance for the proliferation of fragmented instruments and uncoordinated efforts can hinder cross-institutional and data integration and

sharing. Taking an anticipatory approach can help to identify risks and trends in order to implement the needed regulatory action to foster public sector readiness to change.

Box 2.5. Anticipatory innovation governance

As digital transformation is speeding up and new and unforeseen risks emerge due to increased datafication, governments' ability to anticipate and act upon uncertain futures becomes increasingly important. An important distinction between concepts has to be made:

- Anticipation is the process of creating knowledge – no matter how tentative or qualified – about the different possible futures. This may include, but is not limited to, developing not only scenarios of technological alternatives, but also techno-moral (value-based) scenarios of the future (Nordmann, 2014[58]).
- Anticipatory governance is the process of acting on a variety of inputs to manage emerging knowledge-based technologies and socio-economic developments while such management is still possible (Guston, 2014[59]). This may involve inputs from a variety of governance functions (foresight, engagement, policy making, funding, regulation, etc.) in a co-ordinated manner.
- Anticipatory regulation is a function of anticipatory governance which uses regulatory means to create space for sandboxes, demonstrators, testbeds, etc. for various technology options to emerge. This requires an iterative development of regulation and standards around an emerging field (Armstrong and Rae, 2017[60]).
- Anticipatory innovation governance is a broad-based capacity to actively explore options as part of broader anticipatory governance, with a particular aim of spurring on innovations (novel to the context, implemented and value shifting products, services and processes) connected to uncertain futures in the hopes of shaping the former through the innovative practise (OECD Observatory of Public Sector Innovation (OPSI), 2019[61]).

Consequently, anticipation does not mean predicting the future, but is rather about asking questions about plausible futures, then acting upon it by creating room for innovation (e.g. through regulation) or through creating the mechanisms to explore different options in government itself. Most governments today do not have a system in place for anticipatory innovation governance (usually mechanisms connected to the former are siloed under specific policy fields or functions, e.g. foresight). This, in face of increased datafication, is, however, extremely important as choices made today regarding the ownership, interoperability, privacy and control regarding data will influence analytics and services that will be built on the data that cannot be predicted or foreseen today. For the latter, different mechanisms to explore possible futures are needed. To this end, the Observatory of Public Sector Innovation has launched an Anticipatory Innovation Governance Project in which, together with leading countries, the OECD will test out in practice different mechanisms for anticipation.

Source: Information provided by the OECD Observatory of Public Sector Innovation.

Across OECD member and partner countries, examples of regulatory instruments related to data governance are vast. These instruments cover different policy issues from data sharing and interoperability to open government data. Examples of regulation related to data protection are provided in Chapter 4.

In **Brazil**, the central government is advancing on the development of a new data-sharing decree which will help to improve clarity in relation to the different levels of permitted access to government data [including: full access, partial (restricted to only a few public sector organisations and bodies), protected data (data access rules are defined by the custodian)]. Data sharing is clearly identified as one of the

foundational principles of Brazil's Digital Governance Strategy towards more integrated public services, data openness and the creation of value for citizens (OECD, 2018[62]).

In the **United Kingdom**, the 2017 Digital Economy Act helped to bring further coherence and streamline data-sharing practices in the public sector with a resulting positive impact on citizens, including, for instance, by eliminating the vast range of previous legal gateways blocking data sharing among public sector organisations in the context of fuel poverty payment requests and payments (Roberts, 2019[63]).

Also in 2017, **Italy** developed a set of technical regulations on the territorial data of public administrations, in adherence with the EU INSPIRE Directive. Italy also developed a national metadata catalogue as a fundamental tool for guaranteeing the discoverability and clarity of spatial data and related services. Italy has also implemented a more stringent regulatory framework to safeguard personal data and protect the public administration's data. These regulations, framed in the context of the Digital Administration Code and the Three Annual Plan for ICT in the Public Sector, define a set of security measures issued by the Agency for Digital Italy to evaluate and improve the digital security of the public sector.

Often softer legal and regulatory instruments, such as codes of practice, recommendations or guidelines, follow these instruments.

As described in the OECD *Open Government Data Report* (OECD, 2018[6]), countries have also made advancements in establishing the right legal and regulatory environments for open government data. Recent examples include the 2016 Digital Republic Law (Loi pour une Republique Numerique) in **France**, the 2016 Basic Act on the Advancement of Public and Private Sector Data Utilisation in **Japan** and the 2017 Law for the Promotion of E-government in **Germany** (OECD, 2018[6]). Executive decrees on open government data are also available in **Argentina, Brazil, Mexico** and **Peru**.

Box 2.6. Argentina, France and Italy: Soft law instruments for data interoperability and quality

Argentina: Guide for the Identification and Use of Interoperable (data) entities

As part of several efforts to bring order to data management and sharing practices within the Argentinian public sector, the National Direction of Public Data and Public Information published the Guide for the Identification and Use of Interoperable (data) entities. The guide is an ongoing effort to ensure that both public and private sector organisations can follow simple methods to generate, share and/or consume good-quality government data, therefore putting the data as a service vision in practice.

It provides guidance on how to produce simple identifiers for data that are produced by different public sector organisations, but that at the same time are regularly shared among organisations (e.g. country > country_id). Consistent and increasing efforts have been underway since 2017 to make sure this core reference framework for government data is available through APIs.

France: The General Reference Framework for Interoperability

In France, the General Reference Framework for Interoperability offers a series of recommendations to promote interoperability across information systems within the public sector.

Following the rationale of the European Interoperability Framework, the French framework focuses on different levels of interoperability, setting standards for each level that are to be implemented by public sector organisations. Standards are therefore established for technical, semantic or syntactic interoperability to guarantee that public sector organisations, their dispositions and systems are as interoperable as possible:

- The semantic interoperability refers to the meaning of different words, which often varies among public sector organisations. This interoperability aims to streamline the definition of words

across public sector organisations to ensure there is agreement regarding the meaning of data that are exchanged and on the context of the exchange.

- The technical interoperability refers to data formats and data exchange protocols as well as the conditions and formats of storage of these data. This interoperability ensures that data can be properly exchanged among public sector organisations and in the right format.
- The syntactic interoperability stands as a subset of the technical interoperability as it focuses on the technical format data should have in order to be properly exchanged among public sector organisations.

Italy: White Paper on Artificial Intelligence

In March 2018 Italy published the White Paper on Artificial Intelligence. The white paper recommends that all administrations ensure the quality and usability of the data they provide in order to ensure these data are used to test and refine artificial intelligence systems. Additional tools, modelled to fit the needs of the public administration in relation to the use, interpretation and release of data, are available on the national data catalogue dati.gov.it and the National Guidelines for the Valorisation of Public Information Assets.

Sources: Argentina and France : OECD (2019[3]), Digital Government Review of Argentina: Accelerating the Digitalisation of the Public Sector, https://doi.org/10.1787/354732cc-en. with information from Direction Interministérielle du Numérique et du Système d'Information et de Communication de l'État (2015), Référentiel Général d'Interopérabilité: Standardiser, s'aligner et se focaliser pour échanger efficacement, http://references.modernisation.gouv.fr/sites/default/files/Referentiel_General_Interoperabilite_ V2.pdf) ; Italy: AGID (2018), White Paper on Artificial Intelligence at the service of citizens, Available at: https://ia.italia.it/assets/whitepaper.pdf.

Skills: Capacity building, collaboration and knowledge-sharing

Public sector capacity, talent and collective knowledge are core elements not only of good data governance in the public sector, but also of broader public sector reforms, including digitalisation and innovation efforts. For this reason, OECD instruments such as the OECD Recommendations of the Council on Digital Government Strategies (OECD, 2014[7]) and on Public Service Leadership and Capability (OECD, 2018[9]), as well as the OECD Declaration on Public Sector Innovation acknowledge their value as pillars of transformational and cultural change.

Building greater and systemic public sector capacity has different implications from a public sector data governance perspective, including:

- Purpose (outcome): What for (the policy issue)? Data governance must support the business strategy and achievement of the goals (DAMA International, 2017[26]). This translates into the need for clarity in terms of expected outcomes when implementing data governance initiatives. For instance, while closely related, a capacity-building programme specifically deployed to improve data sharing for public service delivery might differ from one that focuses on promoting ethics and values in the design of public sector algorithms.
- Provider: Who provides support? In earlier stages of data-related initiatives, the support provided to public sector organisations will play a key role in increasing policy take up and awareness. In addition, this support can help to build the right set of skills by providing training towards greater capacity for implementation. For instance, in Mexico, the central government (2012-18) created the Open Data Squad as the government task force in charge of guiding public sector organisations in the process of publishing open government data (OECD, 2018[6]).
- Receiver: Who is the target of capacity-building activities? Good data governance in the public sector is translated into a different set of skills and needs for different groups of public officials, from political appointees or public managers to technicians. In Argentina, the Secretariat of Public

Employment developed a series of skill development programmes that target different groups of public sector employees, for example the Lideres en Acción programme for young officials, and the Construyendo Nuestro Futuro programme for high-level public managers (OECD, 2019[3]). These initiatives complement those in place in the context of the activities of Argentinia's government innovation lab, LABgobar, which focuses on building more technical data skills.

- Assessment: Which skills are needed to achieve the purpose? Better targeting capacity building activities demands an assessment of the current data capacity gaps. An example of this is the National Digital Skills survey conducted in New Zealand in 2017 to assess digital skills in the tech sector and across government. The results of the survey informed the report Digital Skills for a Digital Nation and helped to target capacity-building activities in the country (New Zealand Digital Skills Forum, 2018[64]).
- Coherence: How can public sector organisations standardise the data skill needs? The use of common job descriptions and frameworks improves coherence when attracting talent to the public sector, and promotes inter-institutional mobility and career development. As referenced in earlier OECD work (OECD, 2019[3]), one of the most well-known frameworks for job descriptions in the digital and data domain is the United Kingdom's Digital, Data and Technology Profession Capability Framework.[18]
- Mainstreaming: How to move from learning silos to collective knowledge? Digital and physical platforms and learning environments can help promote peer learning and knowledge sharing. They can also help identify, share and promote the mobility of existent talent within and across the public sector. Canada's cloud-based platform GCcollab[19] is an example of a collaborative digital space that allows public servants, citizens, students and academics to exchange knowledge. The Canadian government has also created an agile model for public workforce mobilisation called Free Agents,[20] which allows public servants to switch job positions across the government for short periods of time, depending on their skill set.
- Openness and engagement: How to leverage the value of external talent and knowledge? Good public sector data governance benefits from acknowledging that public sector organisations are not siloed entities in the data ecosystem. Open knowledge practices and partnerships with actors of the data ecosystem beyond the public sector, such as universities and entrepreneurs, can help build capacity within the public sector and attract talent when needed.

Delivery layer

The delivery layer integrates the set of processes, mechanisms and tools that allow for the operational implementation of data governance at a more granular level.

The data value cycle

The data value cycle (see Chapter 3) is in itself complex, for it is the crossroad of the most strategic and tactical aspects of the data governance (regulations, policies) with those that are more technical (e.g. the architecture and infrastructure supporting data management, sharing, access, control and reuse). For instance:

- Different stages of the data value cycle call for different technical skills and roles (e.g. data custodians, data architects, data scientists). This draws on the different outputs that result from data processing at each different stage. The implementation of training and capacity-building programmes at the tactical level support the growing availability of these skills (see previous section).
- Each stage of the data value cycle faces specific challenges that may require policy actions. For instance, bias can take place in the data collection stage, thereby having negative consequences

on how policies are informed and on the resulting interventions designed using those data as an input. In the United Kingdom, the Department for Digital, Culture, Media and Sports has hosted events focusing on addressing the gender data gap (Roberts, 2019[63]), recognising that data on issues that disproportionately affect women are either never collected or of poor quality. In an attempt to reduce gender bias in data collection, the UK government has developed a government portal devoted to gender data.[21]

- The data value cycle is a continuum of inter-related, not siloed, stages, where different actors add value and contribute to data reuse. For instance, government initiatives that focus on the production of good-quality data can contribute to greater interoperability, sharing and openness in later stages. In Argentina, the data as a service approach aims at securing the production of good-quality and interoperable public sector data (OECD, 2019[3]). By using this tactic, the government facilitates the publication, sharing and reuse of public sector data (including open data) by public entities and external consumers.
- The data value cycle may reflect organisational processes that might be the result of legacy systems. Reassessing or re-engineering these processes is crucial to ensure that digitalisation and data-driven efforts contribute to transformation and avoid the perpetuation of inefficient processes in the digital world.
- Data protection takes place (or should take place) across all different stages with data custodians having a key role in ensuring the trustworthy and protected processing of the data. These officials should also manage risks of data corruption or data leaks (intentional or not) across the whole value chain, which can also have undesired effects on public trust.[22]
- The data value creation process is not linear, but cyclical (value cycle).[23] The idea of a value cycle implies a shift in thinking from the value chain as a linear process to an iterative cycle that benefits from evolution and learning (Cordery, Woods and Collier, 2010[65]). When this rationale is applied to the data value chain, it reflects the whole policy-making process (from definition to its implementation, evaluation and revision); and increases the impact of investments on sound data management practices, for data are continuously produced, analysed, shared, used and reused to inform and evaluate policy.

The relevance of the data value cycle and its implications in the context of governments and public sectors is discussed more in depth in Chapter 3.

National data infrastructures and architectures

Some of the most technical aspects of data governance take place in the context of data infrastructure and architecture. These two elements can help advance data-sharing and management practices across institutions, sectors and borders, and build the foundations for delivering public value (e.g. through better public service delivery).

Estonia's X-tee platform (known as X-Road until 2018)[24] is one of the most well-known examples of a sound data-sharing infrastructure in the public sector. The development and deployment of the X-tee platform set the foundations for real-time data sharing between Estonian public sector organisations. Created in 2001, X-tee implies the implementation of a data federation model that helped build more effective, seamless and streamlined public services.

The value of the X-tee relies on its integrating role. Thus, it aims to provide a whole-of-government solution (government as a platform in practice) to enable the secure and authenticated sharing of data across previously siloed data sources. The use of the X-tee in Estonia is regulated by law and public sector organisations willing to access or share data from or with other public sector organisations are obliged to use the X-tee tool. This helps avoid the proliferation of other data-sharing solutions in the public sector and promotes public sector cohesion in Estonia. These efforts provided a cornerstone that has been crucial to building a digital government, enabling integrated services and platforms within and outside the public

sector, and increasing the benefits for citizens and businesses in the country. Also, the cross-border Estonian-Finnish X-Road platform model has been implemented in other countries such as the Faroe Islands, Iceland, Japan and Kyrgyzstan (E-estonia, 2018[66]).

Another example of the willingness of OECD countries to improve their national data infrastructure is the Data Federation Project in the **United States.**

Box 2.7. United States: Data Federation Project

The US Data Federation Project aims to bring greater coherence to data federation practices in the US public sector in order to better support policy decisions, increase operational efficiencies, enable the diffusion of shared processes and infrastructures, foster an integrated government, and combat silos.

The proliferation of the different data federated models using different tools, processes and infrastructure could therefore be prevented and gradually replaced with a single and scalable data federation model developed by the central government. This would follow a "government as a platform" approach, thus the overall goal is to build a shared tool for data federation that could be adopted across the public sector.

The project will draw on the collection of best practices regarding efforts to collect, combine and exchange data from disparate sources and across different public sector organisations and levels of government. In addition, it aims to establish data standards, offer guidelines and deliver reusable tools such as for automated aggregation in order to foster knowledge sharing across public sector organisations and effective reuse of government data coming from different sources.

Source: Originally published in OECD (2019[3]), Digital Government Review of Argentina: Accelerating the Digitalisation of the Public Sector with information from Lindpainter, J. (2019[67]), "The US Data Federation wants to make it easier to collect, combine, and exchange data across government", https://18f.gsa.gov/2019/03/05/the-us-data-federation.

In an effort to improve its national data architecture and infrastructure, **Italy** developed the National Digital Data Platform. This platform offers big data solutions, including data lakes,[25] to facilitate easy access to, sharing of and analysis of large volumes of raw and unstructured data from the public administration. It demonstrates an increasing understanding among governments of the need to design data infrastructures and architectures adapted to emerging new technologies, including artificial intelligence and machine learning. In the context of open data, the Italian data portal dati.gov.it also responds to the need for stronger collaborative data sharing within in the public sector. It is based on a principle of a "federation of catalogues", which allows for any public sector organisation to "feed" the data catalogue with periodic updates. The catalogue therefore also helps measure the outputs of the open data policy in terms of data availability.

Opportunities for greater openness and collaboration with external actors have emerged as a result of governments' demand for better and more efficient data-sharing infrastructures. For instance, in the **United Kingdom**, the Digital Marketplace[26] project has brought external providers of digital solutions closer to the public sector, by providing resources such as the G-cloud framework,[27] which guides external suppliers of cloud-based services when delivering services to public bodies. Inspired by the UK model, **Norway** has launched a project aiming at creating a similar procurement platform for cloud-based services following its 2016 cloud-computing strategy.[28]

Also, the use of APIs is growing fast across OECD member and partner countries as an effort to integrate data, processes and organisations (including those outside the public sector) in real time. In **Brazil**, the central government's integration platform and API catalogue Conecta.gov[29] allows public sector

organisations to more easily and effectively share data between themselves, facilitating the implementation of the once-only principle (as defined by Brazilian law[30] in 2017).

APIs are also being provided for public access in the context of open government data policies across different OECD countries, including **Australia, Canada, Colombia, Denmark, France, Mexico, Portugal, Switzerland** and the **United Kingdom** (OECD, 2018[6]).

As mentioned in the earlier in this chapter, the Nordic countries of **Denmark**, **Norway** and **Sweden** have all secured stronger policies for base data registers, enabling real-time sharing of public information within (and in some cases outside) the public sector. Realising the benefits of effective sharing of base registers, several other countries are starting to look at similar solutions. In **Brazil**, a new Data Sharing Decree[31]will include the creation of a citizen base register to improve the quality of citizen identification and biographical information and facilitate an end-to-end digital public service.

The need for greater data standardisation has also gained traction across OECD countries not only within the public sector, but also in the context of cross-sectorial and international efforts to foster regulatory compliance, public sector accountability, integrity and citizen engagement. For instance:

- As part of its quest to protect citizens' digital rights and personal information, the **French** National Commission on Information Technology and Civil Liberties (CNIL) created a standard on data protection governance,[32] which comprises 25 technical requirements for private and public organisations managing personal data, in order to comply with the EU's General Data Protection Regulation. Singapore also provides technical guidelines for ethical data sharing between organisations, with its Trusted Data Sharing Framework[33] released in June 2019. See Chapter 4 for a more in-depth discussion on data ethics in the public sector.
- The XBRL[34] digital business reporting standard is an example of a data standard adopted by governments across the world. It allows financial statements and reporting information to move rapidly, accurately and digitally between private and public sector organisations using a common reporting term language, and therefore simplifies regulatory compliance and business reporting. The XBRL standard is today used by governments in OECD countries such as **Germany, Japan** and the **United States**.[35] The SBR project in the **Netherlands** (see Flexibility and scalability earlier in this chapter) is another good example of a country that is applying business reporting standards to cut red tape and improve regulatory compliance through digital solutions.
- Partnerships such as the C5 (which groups **Argentina, Colombia, France, Mexico,** the **United Kingdom** and **Ukraine**) reflect cross-national efforts to spur the definition and implementation of coherent open contracting data practices. This includes the adoption of common international data standards such as the Open Contracting Data Standard, which offers a series of guidelines regarding the release of standardised, high-quality and reusable data and associated documents for each phase of a public contracting process. The recent partnership between the Open Contracting Partnership (leading the Open Contracting Data Standard) and the Infrastructure Transparency Initiative will help to further pave the way for the increased adoption of better data management and open data practices in the context of public infrastructure, and enhance the quality of the Infrastructure Transparency Initiative's Infrastructure Data Standard.

References

Algmin, A. and J. Zaino (2018), *Trends in Data Governance and Data Stewardship: A 2018 DATAVERSITY Report*, DATAVERSITY Education, LLC, http://content.dataversity.net/rs/656-WMW-918/images/Trends%20in%20Data%20Governance%20and%20Stewardship_FinalRP-Graphs.pdf (accessed on 4 September 2019). [14]

Armstrong, H. and J. Rae (2017), "A working model for anticipatory regulation: A working paper", NESTA, London, https://www.nesta.org.uk/report/a-working-model-for-anticipatory-regulation-a-working-paper (accessed on 6 September 2019). [60]

BARC (2019), *Data Governance: Definition, Challenges & Best Practices*, Bi-Survey.com, https://bi-survey.com/data-governance (accessed on 4 September 2019). [28]

BEIS and DCMS (2018), *AI Sector Deal*, Department for Business, Energy & Industrial Strategy and Department for Digital, Culture, Media & Sport, London, https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal. [19]

BZK (2019), *Data Agenda Government (Data Agenda Overheid)*, Ministry of the Interior and Kingdom Relations, https://www.nldigitalgovernment.nl/wp-content/uploads/sites/11/2019/04/data-agenda-government.pdf (accessed on 23 August 2019). [46]

Chiesa, G. (2019), *Technological Paradigms and Digital Eras: Data-driven Visions for Building Design*, Springer International Publishing, http://dx.doi.org/10.1007/978-3-030-26199-3. [2]

CIO UK (2019), *Ordnance Survey Chief Data Officer Caroline Bellamy reveals data strategy*, 20 February, 2019, https://www.cio.co.uk/cio-interviews/ordnance-survey-chief-data-officer-caroline-bellamy-explains-strategy-3692557/ (accessed on 21 August 2019). [34]

Cordery, C., M. Woods and P. Collier (2010), "From value chain to value cycle: The role of risk management and ICT", *SSRN Electronic Journal*, http://dx.doi.org/10.2139/ssrn.1761661. [65]

DAMA International (2017), *DAMA International's Guide to the Data Management Body of Knowledge (DAMA-DMBOK2)*, Technics Publications, https://technicspub.com/dmbok (accessed on 27 August 2019). [26]

DCMS (2019), *National Data Strategy: Guidance*, Department for Digital, Culture, Media and Sports, London, https://www.gov.uk/guidance/national-data-strategy (accessed on 23 August 2019). [49]

E-estonia (2018), *X-Road*, https://e-estonia.com/solutions/interoperability-services/x-road (accessed on 19 October 2018). [66]

Element AI and Nesta (2019), *Data Trusts: A New Tool for Data Governance*, https://hello.elementai.com/rs/024-OAQ-547/images/Data_Trusts_EN_201914.pdf. [18]

Executive Office of the President (2019), *Federal Data Strategy: A Framework for Consistency*, Office of Management and Budget, Washington, DC, https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-18.pdf (accessed on 26 August 2019). [69]

Federal Data Strategy Development Team (2019), *2019-2020 Draft Federal Data Strategy Action Plan*, US Government, Washington, DC, https://strategy.data.gov/action-plan (accessed on 26 August 2019). [48]

French Government (2014), *Décret n° 2014-1050 du 16 septembre 2014 instituant un administrateur général des données*, French Government, Paris, https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000029463482&dateTexte=&oldAction=dernierJO&categorieLien=id (accessed on 26 August 2019). [52]

Fukaya, T. (2019), "Is evidence contributing to public accountability? Evidence from Japan", presentation at the OECD Expert Meeting on Standards of Evidence, Ministry of Internal Affairs and Communications, Japan. [35]

Ghavami, P. (2015), *Big Data Governance: Modern Data Management Principles for Hadoop, NoSQL & Big Data Analytics*, CreateSpace Independent Publishing Platform. [5]

Government of Canada (2018), *Report to the Clerk of the Privy Council: Data Strategy Roadmap for the Federal Public Service*, Goverment of Canada, Ottawa, https://www.canada.ca/content/dam/pco-bcp/documents/clk/Data_Strategy_Roadmap_ENG.pdf (accessed on 28 February 2019). [53]

Groenveld, B. (2019), *Standard Business Reporting (SBR)*, Dutch Ministry of the Interior and Kingdom Relations. [41]

Grosser, T. (2013), *Data Governance: Daten effizienter nutzen (BARC Research Note)*, https://www.sas.com/content/dam/SAS/bp_de/doc/whitepaper1/ba-wp-barc-data-governance-2267466.pdf (accessed on 4 September 2019). [27]

Guston, D. (2014), "Understanding 'anticipatory governance'", *Social Studies of Science*, Vol. 44/2, pp. 218-242, http://dx.doi.org/10.1177/0306312713508669. [59]

Japanese Government (2019), *Toward a New Era of "Hope-Driven Economy": The Prime Minister's Keynote Speech at the World Economic Forum Annual Meeting*, Prime Minister of Japan and His Cabinet, Tokyo, https://japan.kantei.go.jp/98_abe/statement/201901/_00003.html (accessed on 8 July 2019). [4]

Ladley, J. (2012), *Data Governance: How to Design, Deploy and Sustain an Effective Data Governance Program*, Morgan Kaufmann. [29]

Lantmäteriet (2016), *The Swedish National Geodata Strategy 2016-2020: Well Developed Collaboration for Open and Usable Geodata Via Services*, Lantmäteriet, https://www.geodata.se/globalassets/dokumentarkiv/styrning-och-uppfoljning/geodatastrategin/national_geodata_strategy_2016-2020.pdf (accessed on 3 October 2018). [32]

Lindpainter, J. (2019), "The US Data Federation wants to make it easier to collect, combine, and exchange data across government", 18F, https://18f.gsa.gov/2019/03/05/the-us-data-federation. [67]

Mägi, M. (2019), *Data for law making. Presentation in the context of the OECD meeting on Measuring Regulatory Performance. Oslo, Norway. 2019*, Statistics Estonia, Oslo. [25]

New Zealand Digital Skills Forum (2018), *Digital Skills for a Digital Nation: An Analysis of the Digital Skills Landscape of New Zealand*, New Zealand Digital Skills Forum, https://digitalskillsforum.files.wordpress.com/2018/01/digital-skills-for-a-digital-nation-online.pdf (accessed on 27 August 2019). [64]

NIIS (2019), *Nordic Institute for Interoperability Solutions: History of the Institute*, Nordic Institute for Interoperability Solutions, https://www.niis.org/history (accessed on 3 October 2019). [45]

Nordmann, A. (2014), "Responsible innovation, the art and craft of anticipation", *Journal of Responsible Innovation*, Vol. 1/1, pp. 87-98, http://dx.doi.org/10.1080/23299460.2014.882064. [58]

OECD (2019), *Digital Government in Peru: Working Closely with Citizens*, OECD Publishing, Paris, https://doi.org/10.1787/0c1eb85b-en (accessed on 26 August 2019). [23]

OECD (2019), *Digital Government Review of Argentina: Accelerating the Digitalisation of the Public Sector*, OECD Publishing, Paris, https://doi.org/10.1787/354732cc-en (accessed on 24 June 2019). [3]

OECD (2019), *Digital Government Review of Argentina: Accelerating the Digitalisation of the Public Sector*, OECD Publishing, https://doi.org/10.1787/24131962. [56]

OECD (2019), *Digital Government Review of Sweden: Towards a Data-driven Public Sector*, OECD Publishing, Paris, https://doi.org/10.1787/24131962. [22]

OECD (2019), *OECD Integrity Review of Argentina: Achieving Systemic and Sustained Change*, OECD Publishing, Paris, https://doi.org/10.1787/22190414. [36]

OECD (2018), *Digital Government Review of Brazil: Towards the Digital Transformation of the Public Sector*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264307636-en. [62]

OECD (2018), *Open Government Data in Mexico: The Way Forward*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264297944-en. [37]

OECD (2018), *Open Government Data Report: Enhancing Policy Maturity for Sustainable Impact*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264305847-en. [6]

OECD (2018), *Open Government Data Survey 3.0*, OECD, Paris. [50]

OECD (2018), *Recommendation of the Council on Public Service Leadership and Capability*, OECD, Paris, http://www.oecd.org/gov/pem/recommendation-on-public-service-leadership-and-capability.htm (accessed on 12 February 2019). [9]

OECD (2017), *Digital Government Review of Norway: Boosting the Digital Transformation of the Public Sector*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264279742-en. [21]

OECD (2017), *OECD Recommendation of the Council on Public Integrity*, OECD, Paris, http://www.oecd.org/gov/ethics/recommendation-public-integrity (accessed on 30 August 2019). [10]

OECD (2017), “Programme for OECD Expert Workshop: Enhanced Access to Data: Reconsiling Risks and Benefits of Data Reuse”, OECD, Paris, https://www.oecd.org/internet/ieconomy/oecd-expert-workshop-enhanced-access-to-data-copenhagen-programme.pdf. [15]

OECD (2017), *Recommendation of the Council on Health Data Governance*, OECD, Paris, https://www.oecd.org/els/health-systems/health-data-governance.htm (accessed on 22 August 2019). [31]

OECD (2017), *Recommendation of the Council on Open Government*, OECD, Paris, http://acts.oecd.orgRECOMMENDATIONPUBLICGOVERNANCE (accessed on 30 August 2019). [8]

OECD (2016), *Open government data review of Mexico : data reuse for public sector impact and innovation.*, OECD, https://doi.org/10.1787/24131962. [55]

OECD (2016), *Open Government Data Review of Mexico: Data Reuse for Public Sector Impact and Innovation*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264259270-en. [54]

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264229358-en. [68]

OECD (2015), *OECD Public Governance Reviews: Estonia and Finland: Fostering Strategic Capacity across Governments and Digital Services across Borders*, OECD Public Governance Reviews, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264229334-en. [43]

OECD (2015), *Recommendation of the Council on Budgetary Governance*, OECD, Paris, https://www.oecd.org/gov/budgeting/Recommendation-of-the-Council-on-Budgetary-Governance.pdf (accessed on 30 August 2019). [13]

OECD (2015), *Recommendation of the Council on Public Procurement*, OECD, Paris, https://www.oecd.org/gov/public-procurement/OECD-Recommendation-on-Public-Procurement.pdf (accessed on 30 August 2019). [11]

OECD (2014), *Recommendation of the Council on Digital Government Strategies*, OECD, Paris, http://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf. [7]

OECD (2013), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm (accessed on 22 August 2019). [42]

OECD (2012), *Recommendation of the Council on Regulatory Policy and Governance*, OECD Publishing, Paris, https://doi.org/10.1787/9789264209022-en (accessed on 30 August 2019). [12]

OECD (forthcoming), *Open and Connected Government Review of Thailand*, OECD Publishing, Paris. [38]

OECD Observatory of Public Sector Innovation (OPSI) (2019), *Presentation by the OPSI*, OECD, Paris. [61]

Office for Artificial Intelligence (2019), *AI Sector Deal One Year On*, Office for Artificial Intelligence, London, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819331/AI_Sector_Deal_One_Year_On__Web_.pdf. [20]

Office of the Government Chief Information Officer (2019), *Public Service Data Strategy 2019-2023*, Government of Ireland, https://www.osi.ie/wp-content/uploads/2018/12/Public-Service-Data-Strategy-2019-2023.pdf (accessed on 23 August 2019). [47]

Open Data Institute (2018), "Defining a 'data trust'", Open Data Institute, London, https://theodi.org/article/defining-a-data-trust. [16]

Open Data Watch (n.d.), *The Data Value Chain: Moving from Production to Impact*, Open Data Watch, Washington, DC, https://opendatawatch.com/publications/the-data-value-chain-moving-from-production-to-impact (accessed on 16 July 2018). [72]

Ordnance Survey (2017), *Ordnance Survey appoints new chief data officer*, 28 June, https://www.ordnancesurvey.co.uk/about/news/2017/carolinebellamy_chief_data_officer.html (accessed on 21 August 2019). [33]

Roberts, S. (2019), *Data in UK Government*, UK Department for Digital, Culture, Media and Sport, London. [63]

SBR (2019), *What is SBR?*, https://www.sbr-nl.nl/sbr-international/what-sbr (accessed on 22 August 2019). [40]

Sen, H. (2019), *Data Governance: Perspectives and Practices*, Technics Publications LLC, Bradley Beach, NJ. [30]

Stats NZ (2019), *Data Leadership Quarterly Dashboard*, New Zealand Government, https://www.data.govt.nz/about/government-chief-data-steward-gcds/data-dashboard (accessed on 26 August 2019). [51]

Sweeney, K. (2019), "An operational data governance framework for New Zealand government", Stats NZ, Wellington, https://statsnz.contentdm.oclc.org/digital/collection/p20045coll1/id/2657 (accessed on 27 August 2019). [24]

The Economist (2017), "The world's most valuable resource is no longer oil, but data: Regulating the Internet giants", *The Economist*, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (accessed on 28 February 2019). [1]

UK National Audit Office (2019), *The Challenges in Using Data Across Government*, UK National Audit Office, London, https://www.nao.org.uk/wp-content/uploads/2019/06/Challenges-in-using-data-across-government.pdf. [70]

US Congress (2019), *H.R.4174: Foundations for Evidence-Based Policymaking Act of 2018*, US Congress, Washington, DC, https://www.congress.gov/bill/115th-congress/house-bill/4174/text (accessed on 6 September 2019). [57]

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*, OECD Publishing, Paris, https://doi.org/10.1787/19934351. [71]

VRK (2018), *Finland's and Estonia's Data Exchange Layers Connected to One Another on 7 February: The Rapid Exchange of Information Between the Countries Is Now Possible*, Population Register Centre, Helsinki, https://vrk.fi/en/article/-/asset_publisher/suomen-ja-viron-palveluvaylat-liitetty-yhteen-7-2-tietojen-nopea-ja-luotettava-vaihto-maiden-valilla-nyt-mahdollista (accessed on 23 August 2019). [44]

Wuttisorn, P. (2019), *Open and Connected Governance in Thailand*, Office of the National Digital Economy and Society Commission. [39]

Wylie, B. and S. McDonald (2018), *What Is a Data Trust?*, Centre for International Governance Innovation, https://www.cigionline.org/articles/what-data-trust. [17]

Notes

[1] See, for instance: https://www.cessda.eu/News-Events/News/CESSDA/Open-if-possible-protected-if-needed-Research-data-via-DANS.

[2] "*We must, on one hand, be able to put our personal data and data embodying intellectual property, national security intelligence, and so on, under careful protection, while on the other hand, we must enable the free flow of medical, industrial, traffic and other most useful, non-personal, anonymous data to see no borders, repeat, no borders*". Extract from Prime Minister Abe's speech at the World Economic Forum Annual Meeting. For the complete speech, see: https://japan.kantei.go.jp/98_abe/statement/201901/_00003.html.

[3] See, for instance, the case of the French open data portal in OECD (2018[6]) and the case of Mexico's central government partnerships with civil society organisations in OECD (2018[37]).

[4] See, for instance, the work on data collaboratives led by Govlab in the United States: https://datacollaboratives.org.

[5] For more information see: https://www.sbr-nl.nl/sbr-international.

[6] For more information see: https://www.logius.nl/english.

[7] For more information see: https://infrastructurepipeline.org.

[8] For more information see: https://e-estonia.com/solutions/interoperability-services/x-road.

[9] The Overview of public sector data governance practices section provides definitions that explain specific data governance aspects, but it does not intend to provide the reader with a comprehensive set of

descriptions and concepts. For this purpose, the author recommends referencing the available literature on data governance, such as DAMA International (2017[26]).

[10] For more information see: https://www.osi.ie/wp-content/uploads/2018/12/Public-Service-Data-Strategy-2019-2023.pdf.

[11] For more information see: https://www.gov.uk/government/publications/national-data-strategy-open-call-for-evidence.

[12] For more information see: http://grunddata.dk.

[13] For more information see: https://datafordeler.dk.

[14] See, for instance, UK National Audit Office (2019[70]).

[15] For more information see: https://www.data.govt.nz/about/government-chief-data-steward-gcds.

[16] For more information see: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000029470857.

[17] For more information see: https://statsnz.contentdm.oclc.org/digital/collection/p20045coll1/id/2657.

[18] For more information see: https://www.gov.uk/government/collections/digital-data-and-technology-profession-capability-framework.

[19] For more information see: https://gccollab.ca/about.

[20] For more information see: https://apolitical.co/solution_article/how-can-government-get-top-talent-canadas-free-agents-work-where-they-want.

[21] For more information see: https://www.gov.uk/government/publications/gender-database/gender-data.

[22] See, for instance, the case of the National Statistics Office in Argentina in OECD (2019), Digital Government Review of Argentina.

[23] For more information see OECD (2015[68]), Van Ooijen et al. (2019[71]) and Open Data Watch (n.d.[72]).

[24] *"X-tee is a data exchange layer used in Estonia. Until 2018, it was named X-Road in English. Since 2018, however, X-Road is only used to refer to the technology developed together by Estonia and Finland through MTÜ Nordic Institute for Interoperability Solutions. The Estonian X-tee is now also called X-tee in English."* Source: Republic of Estonia Information System Authority: https://www.ria.ee/en/state-information-system/x-tee.html.

[25] DAMA International's Guide to the Data Management Body of Knowledge defines a data lake as *"an environment where a vast amount of data of various types and structures can be ingested, stored, assessed, and analysed"*. For more information see: https://technicspub.com/dmbok.

[26] For more information see: https://www.digitalmarketplace.service.gov.uk.

[27] For more information see: https://www.gov.uk/guidance/g-cloud-suppliers-guide.

[28] For more information see: https://www.difi.no/rapport/2018/08/innkjopsordningmarkedsplass-skytjenester.

[29] For more information see: https://catalogo.conecta.gov.br/store.

[30] Law No. 13,460 of 26 June 2017, available at: www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/Lei/L13460.html.

[31] Information received from the Brazilian government (Secretaria de Governo Digital). The new data-sharing decree is expected to be released in 2019.

[32] For more information see: https://www.cnil.fr/en/what-you-should-know-about-our-standard-data-protection-governance.

[33] For more information see: https://www.pdpc.gov.sg/news/latest-updates/2019/06/first-comprehensive-trusted-data-sharing-framework-now-available.

[34] For more information see: https://www.xbrl.org/the-standard/what/an-introduction-to-xbrl.

[35] For more information see: https://www.datatracks.co.uk/ixbrl-blog/xbrl-around-the-world.

3 The application of data in the public sector to generate public value

This chapter explores the way in which the public sector can recognise data as a strategic asset and apply it in pursuit of public value. It begins by presenting the government data value cycle before discussing how data might be valued as an asset and different approaches that can be taken to understanding public value. The chapter then focuses on the practical ways in which data might be applied to generate public value in three areas: “anticipation and planning”, “delivery”, and “evaluation and monitoring”.

Introduction

The application of data in government has almost limitless potential for providing more efficient, effective and trustworthy public services. Chapter 2 considered the importance of defining and embracing a data governance model that creates the appropriate conditions for a data-driven public sector (DDPS) both at the centre of government and within individual public sector organisations and sectors. The response to this model will be influenced by contextual factors, but all public sector organisations exploring the role of and extracting value from data must clearly define and communicate the purpose to which data are put and the benefits to be achieved. For example, in the **United States**, the Department of Health and Human Services' priority is to create a shareable data environment, while the Navy focuses on enhanced combat capability (US Department of Health & Human Services, 2011[1]; Department of the Navy, 2017[2]).

This chapter will focus on the application of data in the public sector to generate public value. It will first discuss definitions of value, initially presenting the government data value cycle, before going on to explore "valuing data as an asset" and "public value". Having presented a base from which governments can define, argue and realise value, the chapter will develop the framework presented in van Ooijen, Ubaldi and Welby (2019[3]) to discuss how countries are applying data to create, or increase, public value through three types of activity:

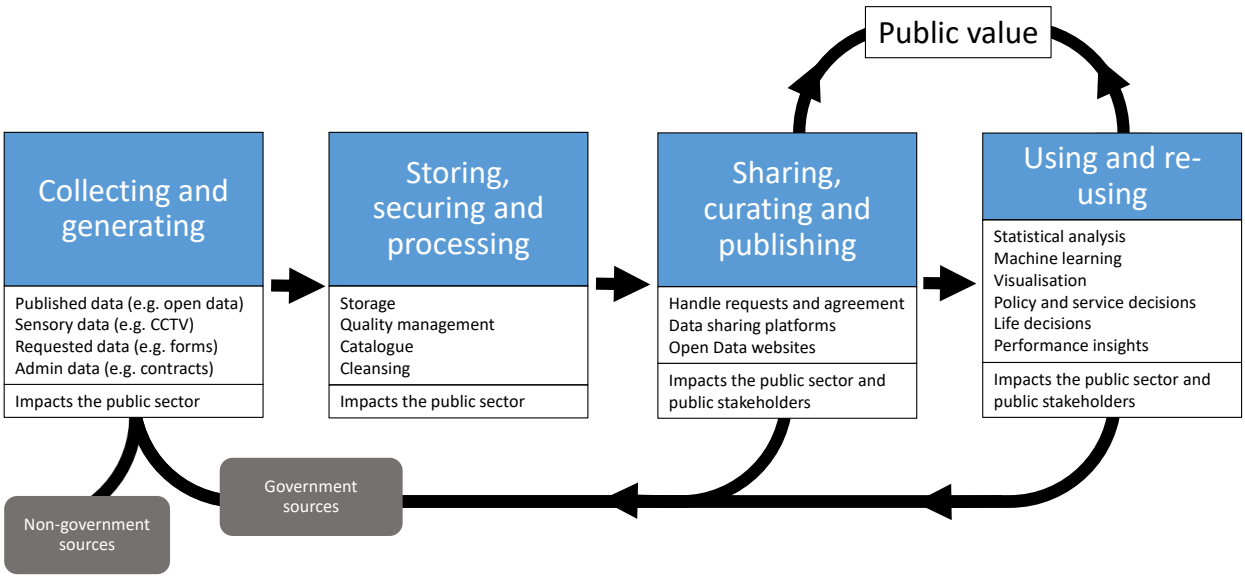
1. Anticipation and planning: The role of data in the design of policies, planning of interventions, anticipation of possible change and the forecasting of needs.
2. Delivery: How the use of data can inform and improve the implementation of policy, responsiveness of government and provision of public services.
3. Evaluation and monitoring: The approach to data involved in measuring impact, auditing decisions and monitoring performance.

Defining value

The government data value cycle

The OECD working paper "A data-driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance" (van Ooijen, Ubaldi and Welby, 2019[3]) presented the idea of the government data value cycle. This cycle identifies the stages through which data pass in order to be managed well and maximise value. The cycle helps track the journey from handling data (raw, isolated and unstructured datasets) to identifying and understanding the relationships between those data, resulting in information and knowledge. The result of such knowledge is the basis for governments to take action and decisions, whether strategic, tactical or operational (Ubaldi, 2013[4]).

Figure 3.1. The government data value cycle



Source: van Ooijen, C., B. Ubaldi and B. Welby (2019[3]), *"A data-driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance"*, https://doi.org/10.1787/09ab162c-en.

Building public sector intelligence in this way allows for the more efficient and effective operation of governments, and the creation of new public value. Nevertheless, it is deliberately presented as a cycle because this change does not happen in a linear fashion, but rather through feedback loops and ongoing iteration. Data can inform and affect the nature of decision-making processes, which in turn can lead to the production and collection of different or more data (OECD, 2015[5]).

This model presents four phases of data in government: 1) the collection and generation of data; 2) the storing, securing and processing of data; 3) the sharing, curating and publishing of data; and 4) the use and reuse of data. The first two stages of the process are entirely about how the public sector manages and looks after its responsibility to the data it generates, collects and holds. As discussed in Chapter 4, this activity touches on several important areas of data rights and the preservation of the public value associated with trustworthy and effective government. The final two stages offer opportunities to generate new public value through ways that will be discussed in the second half of this chapter.

Collecting and generating

This is the starting point for the application of data within government. The data accessed by public servants can take many forms and come from multiple sources. They could involve the consumption of a third party's published dataset, whether as open government data (OGD) or via an application programme interface (API). They could be using the data generated by another piece of technology, perhaps an Internet of Things (IoT) device. They could be data requested as part of the design of a service, like forms collecting information from the public or logged in customer relationship management software following subsequent follow-up enquiries. They could be data produced as the output of government activity, such as one that involved the creation of government contracts. They could also be data held by private sector actors working in conjunction with the public sector to deliver goods and services.

While much of those data are generated by government activity, it is also possible that this first stage in the cycle involves non-governmental sources. This highlights the importance of universal standards in data collection and handling in both the private and public sectors (and forms part of the data infrastructure and architecture discussions in Chapter 2). Although the implications of data involved in this stage are internal

to the public sector and influence internal decisions, having good-quality data helps in its reuse in later phases. As these decisions shape the interactions through which data are collected and lay the foundations for future use, this phase of activity defines the citizen experience of government services (Welby, 2019[6]). As such, public value is a passive by-product rather than, as with later phases, something directly generated from the use or reuse of the data.

Storing, securing and processing

Once data are identified, collected and generated, they must then be stored, secured and processed. This phase of the process is highly important to the discussions covered in Chapter 4 on the role of data and public trust. With data collected, decisions must be taken about how to store it, assess its quality (including any issues around bias), catalogue it and cleanse it. These steps are essential not only in ensuring the confidence of citizens in the public sector's capacity for the proper handling of data, but also in providing a solid basis for the subsequent phases of the cycle.

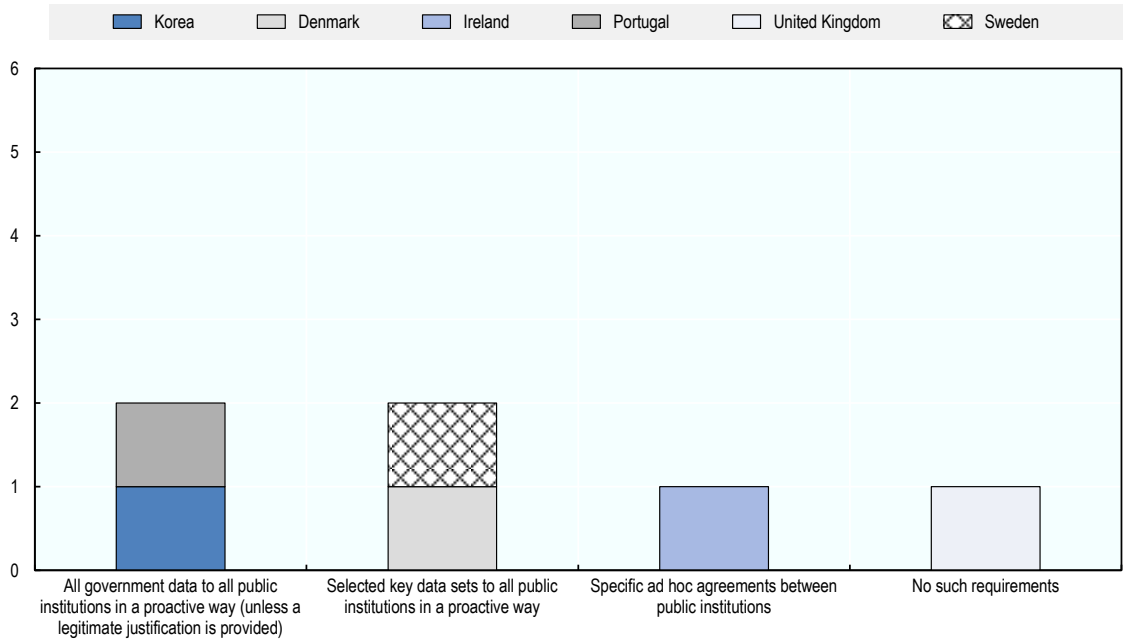
This point of the cycle focuses on the behaviours and activities of those within the public sector in addressing the architectural and infrastructural challenges of high-quality data provision discussed in Chapter 2 considering data governance models. As such, the implications of data involved at the stage of storing, securing and processing are internal to the public sector, influencing internal decisions. They do not create new public value in terms of maintaining trust in government (as covered by the discussions on data-related citizen rights in Chapter 4). Such considerations should especially be a priority for those with responsibility for personally identifiable information, whether they're in the public or private sector.

Sharing, curating and publishing

The third phase of the government data value cycle considers the way in which data that have been stored, secured and processed are shared, curated and published. At this point, legal context and constraints may dictate how readily requests for access and agreements to share can be handled for data that are not openly available. Where there are explicit efforts to support sharing, curating and publishing, the availability of data interoperability platforms and licensing those data that are made available through open data websites should be a priority with the earlier stages of the cycle, thus ensuring the latent quality of data.

The experience of the countries whose participation in the comparative study used as a basis for this report reflects a variety of approaches in terms of how explicit the expectations might be for sharing data between government institutions, especially in order to avoid citizens providing the same information to multiple parts of government.

Figure 3.2. Does your country have an explicit requirement for public institutions to share the data they produce with other public institutions?



Source: Based on information provided by six OECD countries in response to the Questionnaire on the State of the Data-driven Public Sector in OECD Countries, Question 7: "Does your country have an explicit formal requirement (i.e. written guidance provided in an official government document: laws, directives, regulations, guidelines, action plans, executive order, other) for public institutions to share the data they produce with other public institutions?".

In Korea and Portugal, there is a legal expectation for the proactive sharing of data. In **Korea**, the Electronic Government Act provides the legal basis for preventing the duplication of data collected from citizens, thereby requiring the sharing of relevant data within government as a matter of course (Government of Korea, 2017[7]). In **Portugal**, a similar piece of legislation implements the "once-only" principle, meaning citizens do not have to supply same document twice to the government. Portugal's Interoperability Platform for the Public Administration facilitates the exchange of service-related information within government and, following the Resolution of the Council of Ministers 42/2015 of 19 June, extends this to private sector suppliers (Presidência do Conselho de Ministros, 2015[8]).

In Denmark and Sweden**,** only selected datasets are available for all public institutions to access in a proactive way. **Denmark**, similarly to **Argentina's** data as a service approach (see Box 2.6 in Chapter 2), has produced a comprehensive set of resources that detail how to construct and publish data models.[1] These resources allow for a common language for discussing Danish data and simplify its reuse by those wishing to do so. **Sweden** has had a long-standing legal commitment to sharing data, with legislation passed in 1998 detailing which pieces of information are to be shared and the circumstances under which to do so (Finansdepartementet S3, 1998[9]). In **Ireland**, different public institutions come to ad hoc agreements about sharing or accessing data. However, there are ongoing efforts to expand the legislative framework on the reuse of data to establish a more formal model for this. The **United Kingdom** does not have any formal requirements for data created by one organisation to be shared by another, with the implication that data-sharing happens only due to ad hoc requests rather than a strategic approach to interoperability and ease of sharing.

Almost all these countries are taking steps to ensure the publication of data through open data websites providing access to a wide range of datasets. The focus on producing good-quality data early in the government data value cycle to support its reuse later either elsewhere in government or as OGD is

discussed in Chapter 2. However, the internal discoverability of these data is less sophisticated, with only **Korea** and the **United Kingdom** developing a single data inventory for government to simplify the ease with which policy makers and service teams can access these data for reuse. **Denmark**, **Ireland** and **Portugal** have plans for this in the near future while **Sweden** does not.

Internal reuse and discoverability of data is not necessarily limited by the absence of a single data inventory. Neither **Denmark** (Box 3.1) nor **Portugal** have such an inventory, but along with **Korea** they have taken practical steps to consider the needs and structure of base data registries. Such canonical records of information provide a foundation for policy and service delivery that simplify the acts of sourcing, and curating, vital datasets. These are also being developed by the **United Kingdom**, but without explicit legislation to underpin them.

Box 3.1. Basic data in Denmark

The 2010 OECD *e-Government Study of Denmark* (OECD, 2010[10]) highlighted the importance of providing high-quality basic data registries to support the activity of government teams, but also to stimulate the effectiveness of open government data efforts. Although Denmark had some existing registries, coupled with the necessary legal frameworks, their adoption was limited as they did not reflect the needs of their users.

To move away from pure adherence to the law towards the provision of an enabler that responds to needs, the government undertook a three-year programme for implementing basic data registries in Denmark. This effort revisited the whole approach to data governance within the public sector, including changing the legal framework and building partnerships outside of government to capture views and identify valuable sources of data.

As a result, public authorities in Denmark now register various core information about individuals, businesses, real properties, buildings, addresses and more. This information, called basic data, is reused throughout the public sector and is an important basis for public authorities to perform their tasks properly and efficiently, not least because an ever-greater number of tasks have to be performed digitally and across units, administrations and sectors.

However, basic data also has great value for the private sector, partly because businesses use these data in their internal processes and, partly, because the information contained in public sector data can be exploited for entirely new products and solutions, in particular digital ones. In short, good basic data, which is freely available to the private sector, is a potential driver for innovation, growth and job creation.

Source: Local Government Denmark (2012[11]), *Good Basic Data for Everyone: A Driver for Growth and Efficiency*, https://en.digst.dk/media/18773/good-basic-data-for-everyone-a-driver-for-growth-and-efficiency.pdf.

At this stage in the process, the potential impacts of using data are no longer limited to internal public sector stakeholders, but begin to touch those external to government who can begin to use shared data. The first two phases of the government data value cycle shape the citizen experience and are influential in securing trust in government and maintaining public value, but this stage, and the one which follows, sees the potential to generate new public value from the activity of those with whom data are shared to explore policy impacts and service opportunities.

Use and reuse

The final phase of the government data value cycle focuses on the use and reuse of data, and offers the clearest opportunity for generating visible public value. The previous steps in the cycle are often hidden from view. Yet, they should not be neglected, because if there is not an effective approach to them, efforts

to derive value from the use and reuse of data will be undermined due to poor quality data, incomplete sources, unreliable access and barriers to sharing. Therefore, although the public value from the use and reuse of data is visible, it is only because it is supported by a broader ecosystem of data governance, as discussed in Chapter 2, creating the conditions in which data can be successfully applied.

It is well understood that opening data allows for external stakeholders to generate public value on the basis of these data but, in a data-driven public sector, equal weight and attention are given to the internal experience. By improving the management and application of data at each stage in this process, policy makers and public officials can increase their effectiveness by enhancing their data capabilities and ultimately generating greater public value. The second half of this chapter will discuss in more detail how the use and reuse of data can bring that value and it is suggested that for a DDPS built on the government data value cycle, the value is generated from the outcomes of its final two stages. This can include gathering insight on existing policy activity; understanding the issues facing stakeholders; foreseeing new trends and needs; delivering higher quality services; designing and adapting innovative approaches; monitoring ongoing implementation activities; and managing the resources being used to address a particular challenge.

Valuing data as an asset

That the public sector should invest in its data capabilities seems self-evident, particularly as the virtues of data in the digital age have been broadly acclaimed by data evangelists. Human and technical resources focused on data are a priority in both the public and private sectors, with increasing time and money invested in the capture, management, processing and stewardship of data. There has been a 256% growth in data science jobs over 5 years (Indeed Hiring Lab, 2019[12]). Organisations have an intuitive recognition that spending money on data management saves money and reduces risks.

Those efforts are often able to identify the costs of data-related activities, but have been less effective at identifying the benefits of data use, thereby contributing to primarily seeing data as an expense rather than an asset. The ability for organisations to value the data they hold is therefore diminished if there is not a methodology for viewing it with an equivalence to other key assets, like staff and financial resources.

Indeed, while it is encouraging to hear government actors describe data as an “asset” in strategic documents setting out the goals for their future use of data, those documents are often less descriptive in terms of defining how the value of that asset will be calculated. It is essential for the intuition around data’s value to be replaced by a more robust definition for valuing it and providing the basis for business case investment and benchmarking impact.

In accounting terms, the three essential characteristics of an asset have been identified as (Godfrey et al., 2010[13]; Henderson et al., 2017[14]):

1. Does the asset have service potential or provide future economic benefits, where the benefit comes from the use of the asset or its sale?
2. Is the asset controlled by the organisation? That is to say, does the organisation have the power to benefit from the asset and deny or regulate how others access it?
3. Is the asset the result of previous activity? Has the asset been collected through a process, acquired from a source in some way, or through carrying out some work to develop it?

Data share these characteristics and can therefore be called an asset. However, how should that asset be valued? Data are not tangible assets and their value cannot be measured in the same way. For tangible assets, a measure can be taken in terms of an initial cost, the current market value or a calculated potential for generating future revenue. In the business context, such measurement is a priority, not only to support financial reporting to shareholders, but as the basis for mergers or acquisitions, and the calculation of tax.

Neither the private nor public sectors have yet developed a definitive model for measuring the value of data. This is an area which warrants further research, so it is encouraging to see that the Open Data Institute and the Bennett Institute for Public Policy at the University of Cambridge have recently announced a project to establish a taxonomy for valuing data as a route to identifying it as a foundation of data policy (Nuffield Foundation, 2019[15]). Nevertheless, in 1999, Moody and Walsh proposed seven laws for measuring the value of information (Box 3.2) that are helpful in considering some characteristics that can be quantified. Twenty years after those laws of information were identified, the conversation might now focus on data instead of information (discussed in more detail in Chapter 4), but their analysis remains insightful in identifying some of the practical ways in which the value of an intangible asset can be understood and measured.

Box 3.2. Moody and Walsh's seven "laws" of information

1. Information is (infinitely) shareable

Data are an asset that can be shared between multiple people without any loss to their value. This is different from other assets, where multiple actors hold a proportion of the total value. Regardless of how many people have access to the data, it is as though they had exclusive access to it, meaning that value is cumulative, not apportioned: the greater the access, the greater the benefits. Having this understanding also challenges any behaviours at hoarding or duplicating data because they represent a *loss of value*. Duplication of data limits value because it increases storage costs, the potential for redundancy and risks associated with data quality in maintaining accuracy.

2. The value of information increases with use

Most tangible assets decrease in value the more that they are used, but the opposite is true for data – the more that data are used, the greater the return on investment. This is a particularly important point to consider in offsetting the costs associated with the different phases of the government data value cycle, not only to be clear that the marginal costs of data use are negligible in comparison, but also because it is only when data are used that they have value. Unused data are therefore a liability, incurring costs of storage, maintenance and security, rather than an asset.

3. Information is perishable

The value of data may depreciate over time. The speed at which this takes place depends on the type of data in question. Indeed, it is possible that in the public sector, there are certain datasets whose value may increase after a period, but this is usually through being combined or contrasted with other comparative data.

4. The value of information increases with accuracy

Inaccurate information can be incredibly costly in the context of the public sector. Decisions taken about policies or service outcomes that rely on incorrect data can have serious consequences. Nevertheless, this should not be interpreted as a requirement for an impossible standard of accuracy, but an important facet in developing a mechanism for valuing data as an asset.

5. The value of information increases when combined with other information

An important mechanism for unlocking the value of data is ensuring it can be compared and combined with other sources. The challenge of interoperability within the public sector can be an impediment to realising the full value of data both in preventing potential benefits and in adding costs by efforts to extract and reconcile different sources instead.

6. More is not necessarily better

With most assets, the more you have, the "wealthier" you are. The inverse is true for data, with increasing proliferation causing greater challenges in allocating limited resources.

7. Information is not depletable

In general, the more an asset is used, the less there is. However, data can often be self-generating: the more they are used, the more that exists. The value of the original data persists, plus the value of what has been derived from it through the process of further analysis and use.

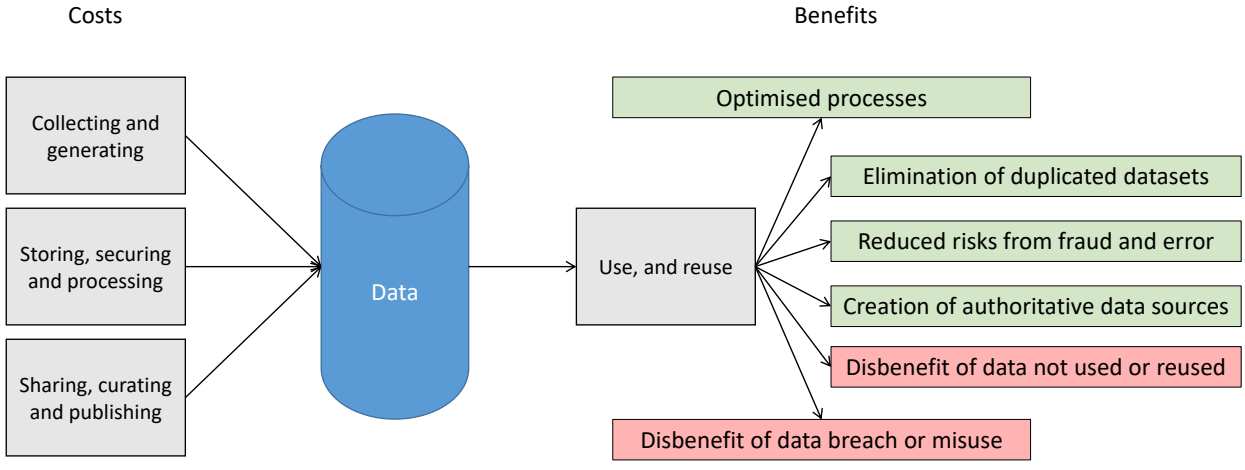
Source: Moody, D. and P. Walsh (1999[16]), *Measuring the Value of Information: An Asset Valuation Approach*, http://si.deis.unical.it/zumpano/2004-2005/PSI/lezione2/ValueOfInformation.pdf.

Despite the challenges of treating an intangible asset in this way, it is important for public sectors to develop practical ways for identifying the value of data. As Ladley, in his book *Making Enterprise Information Management (EIM) Work for Business* (2010[17]), argues, "until data, information, and content are managed as other assets are managed, neither information nor data nor content has a chance to fulfil its potential within organisations".

In doing this, the government data value cycle can provide a valuable way for disaggregating data-related activity into its constituent phases. By considering the costs and benefits associated with each of the four stages (collection and generation; storing, securing and processing; sharing, curating and publishing; and use and reuse), it becomes possible to define value. It is possible to assign data a cost in terms of how much effort is involved in obtaining and maintaining the data. It is also possible to assign a value to the utility of data in terms of where, by whom and how often it is used. This view minimises an understanding of data at rest in favour of reporting on and understanding those involved with using data and the applications to which it is being put. One approach to this could be the use of an internal balance sheet for tracking the value and activity associated with data assets (Laney, 2017[18]).

An approach to identifying the value of data in the public sector on this basis is shown in Figure 3.3. The left-hand side highlights the three areas in which costs are most likely to be incurred while the right-hand side shows the four positive benefits (in green) of using and reusing data and two disbenefits (in red) that would arise from data being poorly used or mishandled.

Figure 3.3. Using the government data value cycle to identify the value of data



This exercise may highlight the priority of addressing some of the "data governance" issues discussed in Chapter 2. In the context of realising the value of data, it is important to get the foundations right so that countries are able to use existing data well as discussed in the OECD *Digital Government Review of Sweden* and the OECD *Primer on Artificial Intelligence* (OECD, 2019[19]; OECD Observatory of Public Sector Innovation, 2019[20]). These efforts can then support the opportunities offered by emerging technologies and ongoing delivery to provide transformed outcomes and unlock the latent value of their data (Ubaldi et al., 2019[21]). Chapter 2 identifies the prerequisites to be addressed in order for each phase of the government data value cycle to operate efficiently.

Using the government data value cycle as the basis for mapping data flows and understanding the sources and use of data helps to identify existing data held within an organisation and the situations in which data are not being used well. The DDPS is not focused solely on developing new services or processing the new scale of data provided by sensor data. Navigating and maximising the value of data that are already held within government is of critical importance. Indeed, there are increasing costs associated with storing, protecting and securing ever-greater quantities of data. In fact, Laws 2 and 6 of Moody and Walsh's suggested laws of information (see Box 3.2) highlight the potential value of data to diminish if they go unused or are collected simply for the sake of doing so.

It is also important to recognise data as an asset in order to secure the trustworthiness of government and data itself (see Chapter 4 for more detail). This need forms the basis for the OECD *Recommendation of the Council on Enhanced Access to and Sharing of Data* being developed under the joint responsibility of the Committee on Digital Economy Policy, the Committee on Scientific and Technological Policy, and the Public Governance Committee. Data must be given an appropriate value in order to ensure that organisations give sufficient attention to securing and protecting it. Following the introduction of the European Union's General Data Protection Regulation, organisations that do not take sufficient steps to secure their data will face significant penalties. Therefore, another way of establishing the value of data as an asset is in the value associated with the repercussions of a data breach.

Treating data as a valuable asset does not mean gathering more and more data or applying it indiscriminately. It means managing and being intentional in how value will be generated. This underscores the importance, discussed in Chapter 2, of knowing what is being gathered; who is gathering it; and the purpose behind any generation, collection, storage or sharing. Every other asset in an organisation is audited and identified, so it is critical that similar activities are carried out in order to understand how data are being treated as well as consideration for the ethical dimension (discussed in Chapter 4).

Establishing a case for data as an asset may prove valuable in helping to implement and establish a data-driven culture throughout the public sector by challenging organisational leaders to appreciate that their data will increase, or decrease, in value directly in relation to their efforts to manage and apply it. In pursuing the development of the DDPS, key performance indicators should be created for those with responsibility for the data agenda that set clear expectations for identifying ways in which data add value, and tackling any lost opportunities in terms of transforming a service or avoiding costs.

In conclusion, it is possible to attempt to measure data in the same way as something tangible. However, while a similar analysis in terms of cost, market value and potential for increased financial returns could be carried out, this is just one factor alongside the role and contribution of data in terms of offering greater accountability, measuring the effectiveness of a particular policy or service, or justifying investment in new and existing interventions. Therefore, any discussion of the value of public sector data must take place in the context of understanding how its usage generates public value, rather than simply as a latent asset. The next section will discuss this concept in terms of the generation of "public value" envisaged by the government data value cycle.

Public value

Having established that the government data value cycle provides the basis for thinking about the role and application of data within a DDPS, and explored how data might be defined and valued as an asset, the final part of understanding the value of data in the context of this chapter is in relation to the definition of "public value".

According to the government data value cycle, it is in the final two stages that new public value is generated; that is in the sharing, curating and publishing of data as a raw material that allows for the use and reuse of that data to create or enhance something else. This could be either as OGD with an expectation of value to be generated by non-government actors (business, academia or civil society) or as data sharing internally within government to obviate the need for citizens to provide the same information to multiple parts of government. In this respect, the conversation about applying data to generate public value looks at the relationship between data as an input and its subsequent outcome.

The origins of the concept of "public value", that is, the value an organisation contributes to society, can be traced to Moore (1997[22]), who wanted to find an equivalence to the private sector's shareholder value within public management. His definition equated public sector managerial success with initiating and reshaping public sector activity in ways that increase its value to the public. Moore's original work emphasised the importance of three particular areas of performance for public agencies:

1. delivering actual services
2. achieving social outcomes
3. maintaining trust and legitimacy of the agency.

This perspective has been complemented by the work of Meynhardt (2009[23]), who suggests that public value is created when there is an impact on a shared experience in terms of the quality of the relationship between the individual and society. While Talbot (2011[24]) emphasises the importance of the public's perspective on what is valuable and important, public value is not declared by governments, but rather defined by what citizens understand to have gained.

The concept of the DDPS is based on the idea that the application of data can generate public value. In this context, there are several organising principles about how that value might manifest itself within these overall categories of delivering services, achieving social outcomes, and maintaining the trust and legitimacy of an agency.

Gross domestic product

One of the traditional ways of measuring the health and happiness of a country is to use gross domestic product (GDP). Using the size of a country's economy as a proxy for the wealth of households and therefore the well-being of society has been a long-standing mechanism for understanding whether or not policies are proving successful at meeting political objectives. Although citizens do not necessarily directly acknowledge the impact of increased GDP, it is one of the areas in which the public value of data could be understood in terms of the financial benefits it might produce.

As discussed earlier, financial value is often the easiest way of defining the value of a tangible asset. In the case of data, that financial benefit has often been cited in terms of making the case for its greater use or release to the public. In **Spain**, the National Observatory of Telecommunications and the Information Society (ONTSI) publishes a yearly assessment of the "infomediary" sector of the economy, businesses that exist because of data. In 2016 ONTSI calculated that by 2015 OGD had generated an impact between EUR 600 million and EUR 800 million. In 2019, the Multisectoral Information Association reported the turnover for these businesses at EUR 1 796 million (ASEDIE, 2019[25]; OECD, 2018[26]).

The financial value of data has been a priority when it comes to making the argument for releasing OGD. In the 2017 OECD Open, Useful and Re-usable data (OURdata) Index (OECD, 2017[27]), 32 out of the

34 participating countries released government data in order to create new business opportunities for entrepreneurs and students. Certainly one of the great hopes of the OGD agenda has been the ambition to use these data to stimulate economic growth through the creation of new industries and business models and the jobs that would follow (OECD, 2018[26]). In the **United Kingdom**, the opening up of geospatial data through the Ordnance Survey's OS OpenData™ initiative was identified as creating a benefit of GBP 8.1 million to GBP 18.2 million in productivity gains and GBP 4.4 million to GBP 8.3 million in additional real tax revenues (ConsultingWhere Limited and ACIL Tasman, 2013[28]). This is fairly modest compared to **Canada's** 2015 assessment of the economic impact on the country's GDP of opening geospatial data to be CAD 695 million (Hickling Arthurs Low Corporation, 2015[29]). Nevertheless, even though that figure sounds significant, it represents just 0.04%, so the GDP financial benefits of data perhaps remain somewhat elusive.

Government efficiency

The efficiency and effectiveness of government services is another means by which public value can be understood. In keeping with the definitions of public value advanced earlier, the increased efficiency of services can be directly experienced by citizens in their day to day lives as a result of digital government approaches (Welby, 2019[6]). Sometimes the citizen will directly experience the improvements to a service following the application of data. In other cases, a citizen may not be aware of the transformative impact of data on their services because government is able to proactively respond to their needs before they make a request or obviates the need for them to supply information because it has been accessed elsewhere in government. Such benefits result in time saved for citizens, but also in reduced back office processing and handling time for public servants too, resulting in increased throughput, fewer errors and greater cost efficiency from an operational point of view. Pollock (2010[30]) concludes that as well as the benefits in generating new products and services built with public sector information or those derived from developing complementary services and consultancy, data can provide indirect benefits, such as reduced transaction costs and increased efficiency of up to GBP 600 million per year.

The **United States** President's Management Agenda (United States White House, 2018[31]) identifies a long-term vision of recognising government data as an asset. Public value is seen in modernising the federal government to improve the ability of agencies to deliver mission outcomes, provide better public services and steward taxpayers' money.

Public sector efficiency gains are considered by several academics whose work has touched on the value of publishing OGD and is discussed in the OECD *Open Government Data Report* (OECD, 2018[26]). This aspect of public value is seen in how making OGD freely available reduces the overheads for organisations in disseminating this information as well as increases the more timely access to information. For others, efficiency is seen less as the external value of improved services and more in terms of cost savings and the improvement of internal processes. At a country level, the recognition that OGD can increase the efficiency of services was acknowledged in the 2017 OURdata Index (OECD, 2017[27]), with 31 of the 34 participating countries stating an intent to improve public sector performance through the release of data (OECD, 2018[26]). In **Luxembourg**, many datasets have been opened for public use, but its main users have been within the public sector itself. Historically, a lot of geodata (cadastre, aerial imagery, topographic maps, address register) were licensed at cost between different public sector bodies, but by removing this cost and opening the data, they can be more widely used, generating increased public value.

The McKinsey Global Institute has calculated potential efficiency gains at EUR 250 billion per year within the European public sector (Manyika et al., 2011[32]) and between USD 35 billion and USD 95 billion per year in the United States by 2020 (Lund et al., 2013[33]). The private sector can also provide a guide in terms of defining the potential productivity gains in a data-driven approach with McAfee and Brynjolfsson (2012[34]) finding that such companies were, on average, 5% more productive than their competitors.

Social value

The previous two definitions of public value have tended to be rooted in financial measurements, but if public value is only defined as GDP and focused on efficiency, then it would be simply "economic value". A 2006 study by the Center for Technology in Government (Cresswell, Burke and Pardo, 2006[35]) found that the ability of government to realise the full value of money spent on IT investment cannot be solely measured in terms of financial results. Instead, the experience they found in five case studies from **Austria**, **Israel** and the **United States** saw that the value of government spending existed in the broader political and social returns to the public at large rather than just the internal value to government operations (as discussed above).

In the **United Kingdom**, HM Treasury issues guidance to public servants on how to construct business cases. As well as setting out the expectations for how investment might be secured, *The Green Book* calls on public servants to focus on the generation of "social value" in its framing of any costs and benefits (Box 3.3). Together with the public value framework (HM Treasury, 2019[36]), a tool for understanding how well public money is turned in to policy outcomes, these are important contributions from a usually financially focused body to broaden the perspective on defining value.

Box 3.3. A classification of costs and benefits in the appraisal of social value from the United Kingdom's *Green Book: Central Government Guidance on Appraisal and Evaluation*

Costs in the appraisal of social value

- Total direct public costs (to originating organisation):
  - capital
  - revenue
- Total indirect public costs (to other public sector organisations):
  - capital
  - revenue
- Wider costs to UK society:
  - monetisable, including cash costs
  - quantifiable but unmonetisable costs
  - qualitative unquantifiable costs
- Total risk costs (the costs of mitigating or managing risks):
  - optimism bias (decreased as estimated risk costs are included)
  - estimated or measured risk cost

Benefits in the appraisal of social value

- Direct public sector benefits (to originating organisation):
  - cash-releasing benefits
  - monetisable non-cash releasing benefits
  - quantifiable but not monetisable benefits
  - qualitative unquantifiable benefits
- Indirect public sector benefits (to other public sector organisations):
  - cash-releasing benefits

- monetisable but non-cash releasing benefits
- quantifiable but unmonetisable benefits
- qualitative unquantifiable benefits

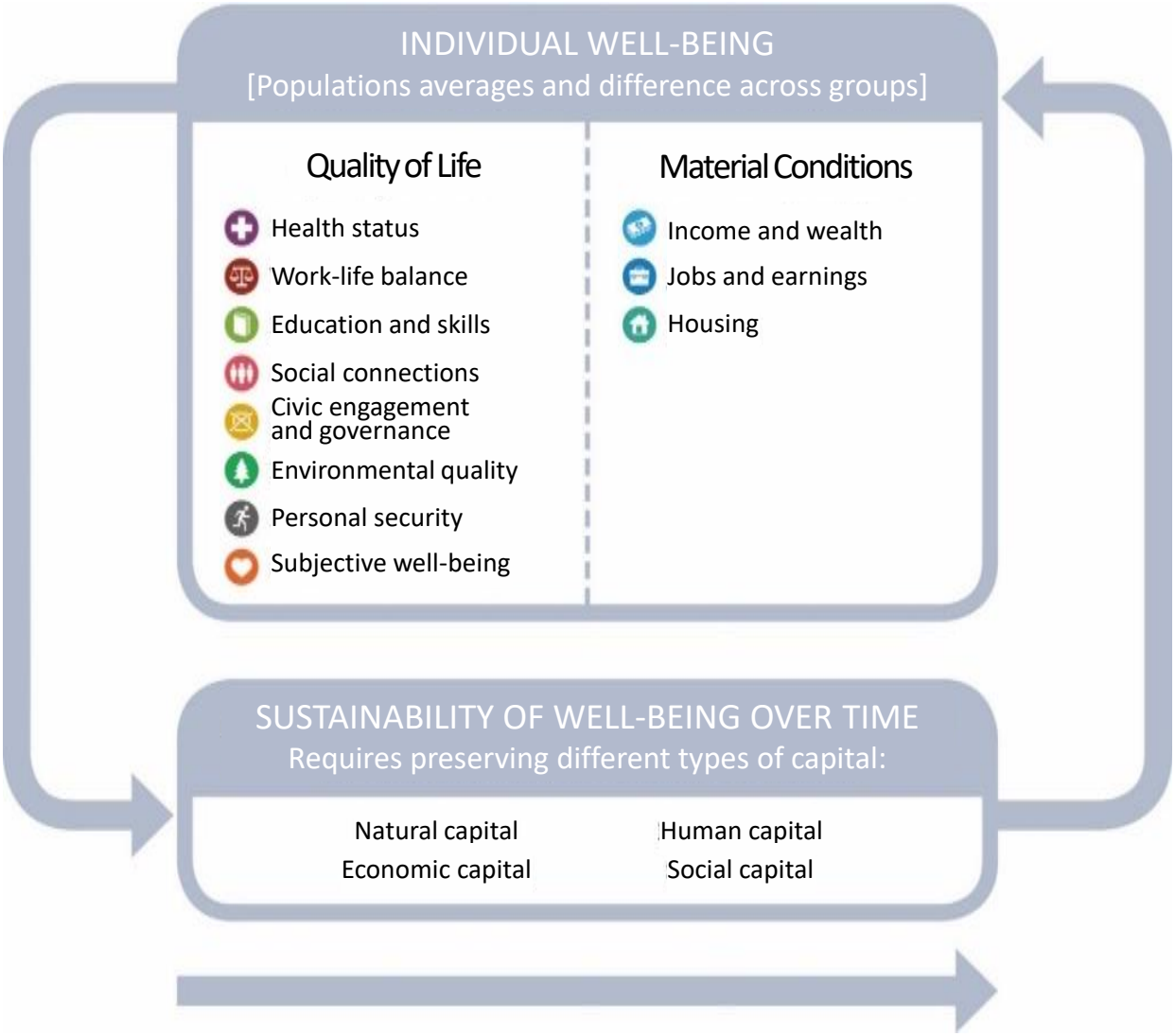
- Wider benefits to UK society (e.g. households, individuals, businesses):
  - monetisable, including cash benefits
  - quantifiable but not monetisable benefits
  - qualitative unquantifiable costs and benefits.

Source: HM Treasury (2018[37]), *The Green Book: Central Government Guidance on Appraisal and Evaluation 2018*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/685903/The_Green_Book.pdf.

The OECD has had a long-standing effort to develop measures for understanding both trust and well-being as part of the Better Life Initiative. The well-being framework (Figure 3.4) shifts the focus away from aggregated economic conditions towards a definition of social progress. It does so by looking to identify the impact of public policies in terms of outcomes rather than purely because of inputs and outputs (OECD, 2017[38]). This results in a blended approach that considers the objective, and subjective, aspects of life and an approach that considers the distribution of experience across a population, thereby incorporating questions of inequality and sustainability into the definition of well-being.

The **New Zealand** government has taken the radical step of rethinking its approach to public spending and is moving away from the pursuit of GDP growth to instead focus on well-being. The country's 2019 budget requires all new spending to go toward five specific well-being goals: 1) bolstering mental health; 2) reducing child poverty; 3) supporting indigenous peoples; 4) moving to a low-carbon-emission economy; and 5) flourishing in a digital age. It uses a living standards framework that is built from citizen level data and tracked with concrete indicators. This builds on a long-standing interest in that country in exploring the possibilities of "social investment" (Acquah, Lisek and Jacobzone, 2019[39]).

Figure 3.4. The OECD well-being framework



Source: OECD (2017[38]), *How's Life?: 2017 Measuring Well-being*, https://dx.doi.org/10.1787/how_life-2017-en.

Engagement and participation

Central to the definitions of "public value" referenced above are citizens and their understanding and participation in the value that is created. Therefore, the application of data to generate public value is not only about making the data available, whether as OGD or in its role in providing public services, but also ensuring that it can be understood and seeking the engagement and participation of citizens.

The ambition for increased transparency and greater accountability of government through the publication of OGD has been an important factor in its success (OECD, 2018[26]). The publication of OGD and the communities that have emerged around particular themes and policy sectors demonstrate that it has created public value in terms of citizen engagement and participation. Chapter 4 will go into more detail about the role of data in building public trust, and highlight ways in which governments can provide effective consent mechanisms for helping citizens to understand the specifics of how their data are being used. While this is important at a technical level, there is also a role for increasing the data literacy of the public and exploring innovative ways of incorporating their perspectives.

An emerging trend in the assessment of public value that looks at engagement and participation and is relevant to the application of data are "mini-publics". "Mini-publics" are "a group of citizens, demographically representative of the larger population, brought together to learn and deliberate on a topic in order to inform public opinion and decision-making" and may take the form of a citizen jury, a consensus conference, deliberative poll or citizen assembly (Breckon, Hopkins and Rickey, 2019[40]).

The example of **Ireland** (Box 3.4) offers insight into how this process blends the application of data in evidence-based policy making with the generation of public value. Randomly selected citizens have been brought together to work through the issues and implications of politically challenging and sensitive topics. This necessitates good facilitation between citizens and experts in order to help engage with evidence and data. It also requires a commitment on the part of the public to fulfil their citizen duties in grappling with complicated issues and considering the broader, societal picture. Where such processes are understood to reflect public participation (and so fulfilling the aforementioned definitions of "public value"), people see any subsequent activity as delivering value, even if it does not follow their personal preferences (Talbot, 2011[24]). However, this means that the value of the exercise owes a lot to the extent to which governments commit to giving "mini-publics" power over the political agenda, similar to the way a judge has to behave in line with the pronouncement of a jury in court.

Box 3.4. "Mini-publics" in Ireland

Ireland first explored the potential of citizen juries in 2012 when the Irish parliament commissioned the Convention on the Constitution. It consisted of 100 members: an independent chair, 29 members of the Irish parliament, 4 representatives of Northern Irish political parties and 66 randomly selected citizens of Ireland.

The Convention was mandated to consider eight specific topics:

1. reducing the presidential term of office to five years, aligning with local and European elections
2. reducing the voting age to 17
3. reviewing the Dáil electoral system
4. giving citizens residing outside the country the right to vote in presidential elections at Irish embassies, or otherwise
5. provision for same-sex marriages
6. amending the clause on the role of women in the home and encouraging greater participation of women in public life
7. increasing the participation of women in politics
8. removal of the offence of blasphemy from the Constitution

as well as an additional two selected by the Convention itself:

9. *Dáil* reform
10. economic, social and cultural rights.

The Convention met over ten weekends of a day and a half. Each meeting had three components: 1) a presentation by experts of papers circulated in advance; 2) debate between groups advocating on either side of an issue; and 3) roundtable discussions involving facilitators and note takers. On Sunday morning, the members considered again the discussions of the previous day and voted on a ballot paper reflecting the details of the debate.

The government formally responded to each of the papers put forward by the Convention, putting three to a public referendum, two of which – an amendment to the Irish Constitution allowing same-sex couples to marry and removing the offence of blasphemy from the Constitution – were passed.

In 2016, following a general election and a new session of the Dáil, a new "mini-public" was formed. The Irish Citizens Assembly again comprised 100 members, including an independent chair, but unlike the Convention, was formed entirely of citizens. Most notable within this session was the debate and recommendation concerning Ireland's ban on abortion. As with the Convention, the Oireachtas did not simply implement the view of the Citizens Assembly, but responded by forming a Joint Committee whose report was enacted and gave the Irish public the ultimate decision via a referendum.

Sources: Breckon, J., A. Hopkins and B. Rickey (2019[40]), *Evidence vs Democracy: How "Mini-publics" Can Traverse the Gap Between Citizens, Experts, and Evidence*, https://media.nesta.org.uk/documents/Evidence_vs_Democracy_Report_Final.pdf; Arnold, T. (2014[41]), "Inside the Convention on the Constitution", https://www.irishtimes.com/news/politics/inside-the-convention-on-the-constitution-1.1744924.

While "public value" can be easily understood at a conceptual level in terms of making an improvement that is understood and recognised by members of the public, it is clear that there are various ways in which that value can be generated. This section has considered the possibility of measuring "public value" through growth in GDP, government efficiency, social value, well-being, or engagement and participation.

There is no single approach for defining "public value" in the application of data, with activities under each of these categories offering different opportunities and routes to realising value. To help identify the most suitable means of defining value, it is important to clarify the reason for seeking to create value, the problem one is trying to solve and the need that needs to be met. One way of ensuring the need is understood from several perspectives is to involve the public and to bring together a diverse, multi-disciplinary team. Delivering successful outcomes and responding to the challenges facing diverse communities requires the collective involvement of external stakeholders as well as those from across policy, delivery and operational teams. This can help to avoid situations where public data are put to uses that diminish public trust and legitimacy while unlocking revolutionary approaches to how governments think about providing services to citizens and how they measure efficiency in service delivery as well as user satisfaction (Welby, 2019[6]).

Understanding, defining and measuring the value of data as an asset and its contribution to public value relies on ensuring the government data value cycle is acknowledged and each step in the process is clearly mapped and measured. Establishing the baselines and benchmarks for the use of data within, and between, government organisations is an important prerequisite for identifying value. Nevertheless, in developing business cases and securing political commitment, often this value needs to be defined on a financial basis. The **United Kingdom's** approach in seeking social value, and discussed in Box 3.3, may be helpful in showing how both financial and non-financial measurements might still be defined in cash terms.

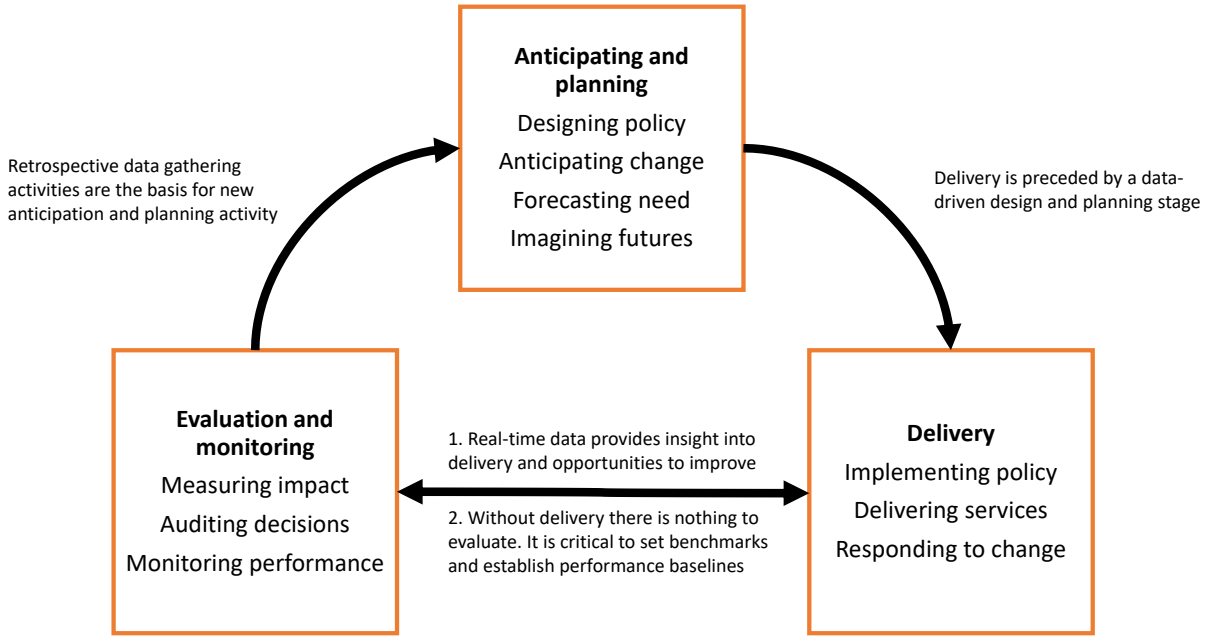
The data governance approach discussed in Chapter 2 is fundamental to the success of DDPS efforts. Ensuring the leadership, capacity to deliver and necessary legal frameworks as well as architectural and infrastructure approaches that enhance the data value cycle should be a priority. Getting this right makes it possible to explore ways for applying data to generate public value, with the confidence that the necessary foundations are in place to achieve successful outcomes and provide a robust measurement of its value.

Applying data to generate public value

A DDPS approach is essential for countries to maximise the potential of digital government approaches for transforming the provision of public goods and services and contributing to increasing citizen well-being. This chapter has discussed a framework for defining the value of data, but the focus will now turn to examples of ways in which data might be applied to take full advantage of the opportunities offered by the DDPS approach.

Van Ooijen, Ubaldi and Welby (2019[3]) propose that the opportunities of DDPS fall into three categories of anticipatory governance, design and delivery, and performance management. One of the aims of this report is to provide an analytical and conceptual framework that can be applied throughout the public sector and across policy areas, to foster more data-driven approaches to policy making and serviced design and delivery. Figure 3.5 proposes an expanded definition that recognises the opportunities for applying data to generate public value as being a broader and more generalised set of three connected and reinforcing behaviours.

Figure 3.5. Where data-driven public sector approaches can generate public value



The first phase is “anticipation and planning”, with its understanding of the role of data in designing policy, anticipating change, forecasting need and imaging future possibilities. This phase focuses on how data can be used to look ahead, whether to anticipate a multiplicity of potential futures or in preparing to take action to resolve a particular problem. “Anticipation and planning” relies on a variety of sources for the data to carry out these activities, including those generated through the evaluation of previous and ongoing interventions.

The second phase, “delivery”, and the activities associated with implementation of policies, the practical delivery of services and the immediate challenges of responding to change focuses on how data are used on an ongoing basis to shape delivery and draw attention to issues that might need an instant response or improve existing delivery modalities. “Delivery” relies on successfully implementing analytical tools and defining effective performance measurements to be able to harness the data that emerge from delivering a service, often in real time, and to quickly and effectively interpret it and apply any resulting insights.

Third, “evaluation and monitoring” in terms of measuring impact, auditing decisions and monitoring performance, is focused on retrospectively analysing events that have taken place and drawing insights from the data generated through the “delivery” phase. As such, there is an important feedback loop between this phase and the “delivery” phase. “Evaluation and monitoring” is a critical source of value in its own right, but also contributes significantly to any associated “delivery” and subsequent “anticipation and planning” efforts that look to learn from previous interventions.

These three areas offer distinct opportunities for applying data to generate value. But as Figure 3.5 showed, there is a flow of data and outputs between them. Therefore, while the remainder of this chapter will consider each phase in turn, this is not to suggest that these are silos with data having value in one

phase only. Instead, these phases should be seen as a continuum, where the application of data in the "anticipation and planning" phase may lead to a set of deliverables, during the "delivery" of which new data will be generated and insights applied and which subsequently will provide the data for the "evaluation and monitoring" of performance and impact. The example of San Francisco's holistic efforts to improve service delivery for disadvantaged youth (Box 3.5) illustrates this. This reflects the ongoing, iterative cycle of delivery that is advocated through a digital government approach of seeing policy, delivery and operations as informing and influencing one another through a multi-disciplinary, cross-sectoral and cross-functional collaboration.

Box 3.5. San Francisco improves service delivery to disadvantaged youth

Sharing data between different organisations within the public sector can be one of the greatest challenges to improving outcomes and delivering public value. In the city of San Francisco, the experience of disadvantaged youth prompted the heads of foster care, juvenile probation and mental health departments to work with the city's attorney to facilitate the limited exchange of case information among the necessary agencies. This transformed the level of care for children interacting with these agencies due to an improvement in case co-ordination and the identification of overlapping clients.

This was made possible thanks to an integrated data system that recognised and focused on the families that were the most vulnerable, most troubled and most in need. As a result of the data integration, it was possible to carry out "evaluation and monitoring" activities that resulted in the realisation that 2 000 users of services consumed half the resources of the department, and that most of those families lived within walking distance. As a result, the Human Service Agency concentrated "delivery" of services in specific neighbourhoods and co-located services at community centres, further increasing efficiency and the quality of service delivery.

As a result of this new linked data source, subsequent "anticipation and planning" efforts were able to be carried out that provided a better assessment of the needs of high-risk youth, identifying opportunities to divert them from damaging future events, understanding where youth were falling through the cracks and establishing what services were needed to intervene earlier to prevent those negative outcomes.

Initially supported by a low-tech system, the system was transferred to a more sophisticated platform to enable the three agencies to better understand the interplay between the data. Creating a shared view of the data highlighted that those clients who were under the care of multiple systems were at higher risk of committing a crime. It found that 51% of San Franciscans involved in multiple systems were convicted of a serious crime, 33% had been served by the 3 agencies, and 88% of these youth committed a crime 90 days after becoming involved with multiple agencies. This offered a critical window of opportunity for the caseworker to intervene and provided the justification for a web-based integrated case management system to make this connection in real time.

Source: OECD (2015[42]), *Rebooting Public Service Delivery: How Can Open Government Data Help to Drive Innovation?*, www.oecd.org/gov/Rebooting-Public-Service-Delivery-How-can-Open-Government-Data-help-to-drive-Innovation.pdf.

Anticipating and planning

The first phase in which countries are demonstrating their ability to apply data to generate public value is in looking to the future in terms of planning, or imagining what might be required to better support their societies. The future is unpredictable and cannot be reliably foretold. There will therefore be scenarios where the necessary data do not, and cannot, exist but decisions will still need to be taken. In those cases, a methodology for identifying public value and understanding the purpose of the intervention and

measuring its impact are helpful in subsequently judging whether or not a decision taken without data has had the desired outcome or not.

Nevertheless, it should always be a priority to attempt to obtain the necessary data for attempting to mitigate the risks associated with the unpredictability of the future. Assuming that such data have been sourced, the "anticipation and planning" phase can begin to see data applied to define and plan an intervention, provide the evidence to support policy-making activity, and the anticipatory governance pursuits of foresight and forecasting. Being prepared to source data in shaping the anticipation and planning of future activity and future needs means countries are able to respond to the unpredictable as well as the planned. Moreover, when governments consider how they might be proactive in responding to the needs of their citizens, it is important that they explore not only related services, but also every opportunity to reimagine the status quo. The ongoing work of the OECD Working Party of Senior Digital Government Officials (E-Leaders) to explore the future of government and collaborate on how to maximise the opportunities of the digital age is an important resource to help governments prepare for, and respond to, these challenges.

In certain policy domains, it will be impossible to source the necessary data. One approach to this scenario is to invite the private sector and civil society actors to share some of the risk. In **Korea**, funding is made available through the "Public sector big data analysis projects" competition to incentivise new ways of applying the insights provided by the country's data to its policy challenges. This provides an experimental freedom to develop models that focus on a particular problem, and which can then be scaled, free from the constraints of the government's own policy and delivery agenda. In the **United Kingdom,** the Land Registry and Ordnance Survey worked with Geovation, the United Kingdom's location and property data lab, to find members of the public with big ideas for transforming society using location or property data and help turn those ideas into viable projects. To date, GBP 23 million has been invested in 84 start-ups across 10 market sectors (Geovation, 2019[43]).

More usually, "anticipating and planning" will be able to identify existing sources of data with which to plan. Sometimes those efforts will have been prompted by a high-profile policy failure, or the prioritisation of a new policy for ideological reasons. Perhaps a think tank, the media or academics will have carried out an analysis of data that shifts the agenda of government. Other times, the evaluation of some ongoing activity and the collection of new data may prompt efforts to target a different outcome. The experiences of **Denmark**, **Ireland**, **Korea**, **Portugal**, **Sweden** and the **United Kingdom** in the research which led to the analysis presented in this report all indicated that when data were used to provide an anticipatory position, it was mostly as a reaction to some existing data or activities with a view to creating a new, forward-looking perspective.

The idea of anticipatory governance is also relevant in the context of innovative public sector data governance, as discussed in Chapter 2.

Evidence based policy making

The first area to consider in terms of the "anticipation and planning" phase is the use of evidence to design policy interventions that respond to forecasted challenges. This is not the same as the forecasting activities (discussed later), which attempt to predict whether or not a policy would be effective. It is about the approaches which countries take to experiment with a particular approach and consider as wide a spectrum of intervention as possible to shape future policy interventions, informed by the availability of data. This is not solely the domain of governments and public servants, as think tanks, journalists and academics are some of the actors involved in thinking through how to respond proactively to the needs of society based on data.

One of the most critical factors in securing the use of data as evidence in pursuit of policy making in the design, implementation and evaluation phases is establishing standards for that evidence. The OECD's

Expert Group on Standards of Evidence has proposed six characteristics (Box 3.6) that should be implemented in order to support evidence-based policy making.

Box 3.6. Ensuring the good governance of evidence: What standards of evidence are needed for policy design, implementation and evaluation?

The OECD Expert Group on Standards of Evidence has developed six standards for evidence:

1. **Appropriateness:** Evidence should be selected to address multiple political considerations, useful to achieve policy goals and consider the local context.
2. **Integrity (honest brokerage):** Individuals and organisations providing evidence for policy making need processes to ensure the integrity for such advice, including managing conflicts of interest, ethical conduct and the influence of lobbying.
3. **Accountability:** Those setting the rules and shape of official evidence advisory systems used to inform policy making should have a formal public mandate, and the final decision authority for policies informed by evidence should lie with publicly accountable officials.
4. **Contestability:** Evidence must be open to critical questioning and appeal, can include enabling challenges over decisions about which evidence to use.
5. **Transparency:** Information should be clearly visible and open to public scrutiny. The public should be able to see how the evidence bases informing a decision are identified and utilised. Transparency is also part of the OECD *Guiding Principles for Regulatory Quality and Governance*, as well as the *Open Government Principles*.
6. **Deliberation:** There should be space for engagement that enables members of the public to bring their multiple competing values and concerns to be considered in the evidence utilisation process. This is also about co-design and co-creation of policies and participation from an open government perspective that contributes to evidence.

Source: OECD (forthcoming[44]), *Standards of Evaluation: A Review of International Perspectives*.

Some countries have developed guidance for public servants on using OGD in the development of policy. According to the 2017 OURdata Index survey, **Austria**, **Colombia**, the **Czech Republic**, **Finland**, **France**, **Japan**, **Korea** and the **United ingdom** have all developed overarching guidelines on how best to use OGD to inform policy-making processes (OECD, 2017[27]). While these countries are providing guidance for public servants, **Denmark**, **Norway**, **Spain** and the **United States** are using OGD to enhance the public debate around policy and develop co-responsibility for responding to its challenges. Moreover, **Chile**, **Colombia**, **France** and **Israel** are hoping the release of OGD will facilitate the crowdsourcing of solutions for public policy problems by tapping into the collective intelligence of the public (OECD, 2018[26]). In **Mexico**, the 2013-18 National Digital Strategy stresses the importance of OGD in contributing to achieving policy outcomes – land management improvement, the digital economy, and natural disaster prevention and mitigation (OECD, 2016[45]).

Korea has developed a standardised model for analysing “big data” within the public sector so that data generated in one part of the public sector can be compared with what is generated elsewhere. The use of the resulting models informs policy making in 18 areas, with 320 standardised models having so far been provided to 175 organisations. There are plans to introduce similar models in categories including citizen services, tourism, transportation, closed-circuit television (CCTV) and public housing. Such standardisation minimises local differences in the analysis which takes place between different institutions, and in particular central and local governments. This allows policy to be informed with a more accurate and comprehensive understanding of a given dataset.

In **Denmark**, significant effort has gone into the handling of education data. A databank and data warehouse provide institutions, regions, municipalities and the public access to a number of predefined reports and graphs with statistics. There is also the possibility for people to define their own reports on certain aspects of the data it contains.

In **Ireland**, the biggest use of data for policy making is in mapping. The Ordnance Survey of Ireland's Geohive service provides easy access to publicly available geospatial data. Combined with data from other sources, these mapping data underpin analysis of housing trends and flood risk. A further development in Ireland is the creation of Pobal, a website and support service providing information on deprivation profiling in a particular area, details of local childcare services and information about other funded services available for people to access. This resource is not only for policy makers, but for citizens and community organisations as well.

One of the most powerful opportunities offered by the application of data in evidence-based policy making is in its potential to support a change in approach. In the Flemish region of **Belgium**, a spending review was carried out with the intent of developing policies that would create jobs in order to meet the needs of the communities. However, the analysis showed that the greatest need was in serving elderly citizens with requirements for domestic services rather than for jobs.

Anticipatory governance

A second area during the "anticipating and planning" phase in which the DDPS approach can generate public value is that of anticipatory governance. Anticipatory governance describes systematic efforts to consider the future in order to inform policy decisions today. In this context, governments respond proactively rather than reactively, based on knowledge and evidence rather than experience and protocol. The use of data leads to the better detection of societal needs as they emerge and improves predictions for future needs. This is a particularly important activity in the context of innovation. The OECD's Observatory of Public Sector Innovation has recently initiated an "Anticipatory Innovation Governance" project to analyse the challenges and opportunities in this space.

Data-enabled prediction and modelling techniques support governments in anticipating societal, economic or natural developments that are likely to occur in the future. They may also capture early warnings and better assess the need to intervene. Additionally, governments that are built on strong data foundations are able to deliver proactive government services that anticipate the needs of citizens and obviate their need to interact with the state, without necessarily realising that has happened.

This reflects macro anticipation at a societal level in terms of understanding emerging trends and carrying out "predictive" activity to inform long-term planning. However, it also reflects the micro anticipation in terms of an individual and their needs. At that level it is not about predicting what an individual is going to need based on their historic choices and presenting them with the existing solution, but about a deeper transformation of the design of the state based on a deep understanding of life events and the sort of interactions that are associated with a given set of services.

Anticipatory governance falls into two categories: forecasting and foresight.

Forecasting

Forecasting in the DDPS context is to use existing data and trends to try to predict the most likely developments and outcomes. Data-enabled predicting and modelling techniques of this sort may support governments in anticipating societal, economic or natural developments that are likely to occur in the future. Forecasting capabilities attempt to spot emerging needs, and anticipate new ones, based on observable trends, be they physical or digital, as in the example in Box 3.7.

Box 3.7. Australia: Predicting hospital patient admissions

The emergency departments of hospitals can often become overcrowded and struggle to respond to patients in a timely manner. Any delay in the care of a patient can increase patient mortality and so Australian hospitals have a target of treating emergency department patients within four hours.

To help hospitals meet this target, the Commonwealth Scientific and Industrial Research Organisation developed the Patient Admission and Prediction Tool (PAPT). Using a hospital's historical data, it can provide an accurate prediction of the expected patient load, their medical urgency and specialty, and how many will be admitted and discharged.

PAPT is now being extended to predict diseases such as influenza and the hospital admissions of patients with chronic diseases.

It is currently in use in 30 hospitals and has shown a 90% accuracy rate in forecasting bed demand. If PAPT were rolled out across Australia, it would equate to AUD 23 million in annual savings.

Source: Dods, S. et al. (2013[46]), *Evidence-Driven Strategies for Meeting Hospital Performance Targets: The Value of Patient Flow Modelling*, https://doi.org/10.4225/08/584c43f4df82b.

In a DDPS, the necessary resources are in place to support forecasting as a mechanism for developing early-warning systems, sentiment analysis of social media and real-time decision support systems (Höchtl, Parycek and Schöllhammer, 2016[47]). The increasing ubiquity of mobile devices and social media platforms means public authorities have a wider range of routes to gather valuable information from citizens related to their daily lives as well as their needs, preferences and behaviours. Taken together, these data allow governments to better assess needs, design more appropriate policy measures and be more precise in estimating an expected impact.

In **Mexico,** the government established Datalab as a specialist data laboratory to develop these capabilities. One area of focus is strengthening anticipatory governance approaches in order to generate data-based predictions of, for example, populations at risk regarding diseases, zones with emerging environmental problems and future arising conflicts (OECD, 2018[26]). Also in Mexico, the Ministry of Energy is using a predictive workforce planning and analytics model to identify current and future talent and skills gaps in critical oil and gas occupations over a ten-year horizon (Deloitte, 2016[48]).

In **Portugal**, funding has been directed towards projects using data science to focus on risk mitigation. One successful project has been analysing the skills of the unemployed labour force compared to the needs of the job market in order to identify those most at risk of becoming long-term unemployed and consequently providing them with targeted training.

Ireland is using social media analytics to model welfare provision and has used predictive data analysis concerning the future needs of the country to support policy associated with Project Ireland 2040, a government-wide exercise to plan for the challenges and opportunities of the next 20 years.

Foresight

In the context of a DDPS, foresight is associated with horizon scanning in order to define problems; it does not attempt to predict the future. It is instead a systematic approach to explore multiple plausible versions of how the future could be different from expected and use those insights to shape policies in ways that can be more agile in responding to them. The most relevant data for foresight processes are those that might identify emerging changes in the present, which could grow into significant and disruptive developments in the future.

The OECD's Strategic Foresight Unit plays an important role in strengthening the capacity of national governments by co-ordinating the Government Foresight Community that consists of over 100 experienced foresight professionals working in governments and international organisations around the world. Additionally, the OECD's Observatory of Public Sector Innovation curates a collection of foresight-related resources within its Toolkit Navigator.[2]

The necessary skills and capacities to carry out successful foresight activities may not always be available, but in **Australia** the Public Sector Innovation Toolkit provides a practical guide to horizon scanning in the public sector. It offers a grounding in what horizon scanning is and how to do it, with checklists and materials to support public servants beginning to apply it in their own context.

Skills and capabilities are not the only prerequisite for successful foresight; the provision of, and access to, the necessary data are too. Furthermore, a foresight mindset requires a commitment to a longer term outlook rather than the short-term political cycles that can sometimes cause policies to focus on immediate issues or demands rather than longer term planning. Given these factors, it is unsurprising that outside the centre of government, foresight activities are more limited. In particular, the OECD/Bloomberg Survey on the innovation capacity of cities indicates that foresight and prospective exercises is an area in which cities are lacking (OECD/Bloomberg, 2019[49]).

Several OECD countries have established institutions that take the lead on exploring the foresight dimension of anticipatory governance. In **Canada**, Policy Horizons operates at the federal level to help the Government of Canada develop future-oriented policy and programs that are robust and resilient in the face of disruptive change. Using the foresight method means that the team takes data from the past and extrapolates it into the future using a variety of tools, from statistics to simulations. In **Portugal**, the Centre for Digital Competencies of the Public Administration (TicAPP) within the Administrative Modernization Agency, has as part of its mission the development of quantitative and predictive models that allow the use of available data to support the political and administrative decision process. Additionally, Portugal also has LabX, an Experimentation Lab for Public Administration created in 2016 to embed a culture of innovation in the Portuguese public administration, (re)designing public services around citizens' needs and expectations, and promoting an evidence-based approach to policy making through testing and experimentation in a controlled environment. The role of labs for policy experimentation and foresight is similarly being explored in the **United Kingdom**, where the Government Policy Lab and the What Works network are two examples of initiatives that look to generate data and then analyse them in order to model different policy scenarios.

Designing services and policy interventions

One of the most compelling opportunities for DDPS is the way in which the application of data can reshape the opportunities for designing better policy interventions and services through a deeper and more rounded understanding of the needs of citizens and engaging citizens as co-creators of value. While this is part of "anticipation and planning" activities, there is a clear linkage between the design and the "delivery" phases.

As countries develop their data governance models (as discussed in Chapter 2) and embed a more sophisticated understanding of the government value data cycle, the use and reuse of data within government becomes more sophisticated. The flow of data around government, its cataloguing and the easing of access to it means that there is the potential for more deeply integrated service design opportunities. Furthermore, as citizens are invited to participate in the design of services and contribute to the user research establishing their needs, services begin to reflect the actual needs and circumstances of citizens.

In the **United Kingdom**, the Government Digital Service has developed a set of mandatory guidelines for assessing and assuring the quality of any public-facing government services. This Service Standard contains 14 points and is administered through a series of assessments at different stages in the implementation cycle. The role of qualitative and quantitative data in understanding the needs of citizens

and their behaviours when interacting with public services is highlighted throughout. Particularly relevant to the role of data in "anticipating and planning" the design of services is the requirement to consider the role of qualitative and quantitative data in ensuring that the responsible teams have understood the needs of their users and are subsequently able to respond to them on an ongoing basis. A similar standard exists in **Canada** with one of its principles requiring Canadian public servants to be good data stewards and collect data from users only once and reuse wherever possible whilst also ensuring that data are managed securely, and in ways that facilitate reuse.

Another important aspect of the design phase of planning for both the "delivery" and the "evaluation and monitoring" of services and policy interventions is the initial effort required in benchmarking performance and measuring success. In order to generate the maximum public value, it is essential to clearly define the purpose of its application; but this is only half the exercise. The other half is identifying how to measure the value and judge the success, or otherwise, of a given intervention.

Box 3.8. 350 000 more organ donors, from just one link

In the **United Kingdom,** citizens can choose to join the organ donation register. The team responsible for increasing its coverage worked with the team responsible for administering the United Kingdom's single government domain, GOV.UK, as well as teams from the Driver and Vehicle Licensing Agency, the National Health Service, the Department for Health, and the Cabinet Office's Behavioural Insights team to explore how they might influence a particular user journey to generate more signups.

The policy need was to increase the profile of organ donation in a sensitive way. To do that, the team ran experiments on the final stage in the journey for people renewing their vehicle tax. In total, they experimented with eight different designs of content and images viewed by in excess of 1 million visitors. As a result, they could identify one of the proposed alternatives was more effective than the original language. In the course of a year, this led to 350 000 more organ donors joining the register.

This example highlights the potential value of exploring nudge-based policy interventions backed up by data capabilities. In this case, the policy team was able to work with a delivery vehicle in the shape of GOV.UK that was responsive to updates and could be used for experimentation. However, it relied on a culture of evaluating data to consider how to improve the approach and maximise both the public return on investment and broader societal value.

Source: Cabinet Office et al. (2013[50]), *Applying Behavioural Insights to Organ Donation: Preliminary Results from a Randomised Controlled Trial*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/267100/Applying_Behavioural_Insights_to_Organ_Donation.pdf.

Delivery

The second phase in which countries demonstrate their ability to apply data to generate public value is the day-to-day activity of delivering services and operating government. As is shown in the case studies accompanying this report, the "delivery" phase is not limited to a focus on services, but reflects a broader perspective that accommodates the role of data in less visible areas of the public sector's work.

As the phase where the most significant interactions between citizens and governments take place, there is an important relationship between "delivery" and the discussion of an enabling data governance model from Chapter 2, the mechanics of implementing the government data value cycle earlier in this chapter, and the implications of data on trust discussed in Chapter 4.

The way in which the DDPS approach manifests itself during "delivery" informs how effectively the value of data can be realised in both the "anticipation and planning" and "evaluation and monitoring" phases.

The link between “delivery” and “evaluation and monitoring” is particularly strong as a DDPS culture will strive to introduce feedback loops that are constantly providing the ability to improve the quality of delivery. These feedback loops, which can be provided by both qualitative and quantitative mechanisms, enable governments to move away from a top-down design and implementation of public services to the formulation of well-targeted service design and need-based policy implementation and service delivery, thereby increasing the reach and effectiveness of services.

Nevertheless, the use of data to shape the “delivery” of government is not always a priority, particularly when it comes to the use of OGD. Most countries view its role in improving public service delivery as secondary, with greater efficiency and effectiveness of services not a main objective of OGD policies and initiatives (OECD, 2018[26]).

The following section will look at how the application of data in the “delivery” phase can generate “public value” in four ways: 1) improving public services that respond to citizen needs; 2) giving public servants the capacity to focus on meeting other needs; 3) communication and engagement with the public; and 4) responding to emergencies, crises and other developing situations.

Improving public services that respond to citizen needs

A DDPS approach enables a closer working relationship between policy design and service delivery activities with a resulting shift from top-down implementation of public services to a user need led approach to design and delivery, based on an end-to-end understanding of a particular service journey, which can consequently increase its reach and effectiveness.

Inclusive user-driven approaches towards government service delivery can be strengthened through the forward-looking approaches highlighted in the previous section on “anticipation and planning”. The analysis of data produced by the behaviour and characteristics of existing users can facilitate predictive activities identifying potential new users and/or emerging needs and problems. While this will inform the development of new services to address unmet needs, there is also the possibility of proactively enhancing the existing approach to address issues in the existing service. As a result, government services can continue to improve, responding to the rhythm of people’s lives and continuously evolving to meet their needs and expectations, in pursuit of delivering greater public value.

Much of the public value that can be generated from developing the use of data in the “delivery” phase of improving public services may take place in ways that are not immediately obvious to an external user. Addressing the regulatory, data architecture and data infrastructure challenges discussed in Chapter 2 offers the potential to transform interoperability of data between government organisations, thereby allowing the prefilling of information and making the once-only principle of data submission a reality. Such efforts can be particularly powerful in reducing the scope of what would be involved in bringing the “long tail” of analogue processes and services on line.

Indeed, the application of data to the delivery of services can accelerate innovation cycles. This is not only because the environment is conducive to experiment with emerging technologies, implemented on a strong foundation of reliable data, but also through more agile design approaches. The Lean Startup (Ries, 2011[51]) approach of build-measure-learn encourages a minimum viable approach to be put in front of users as soon as possible in order to learn and continuously iterate and improve. The embedding of a data-driven approach with this delivery culture means it will be easier for public institutions to know how citizens use their services, or how satisfied they are with them, learn from it, and adapt the design and delivery accordingly.

A further hidden value is the capacity for public service providers to deliver in a proactive way, i.e. to deliver a service before a user has had to engage the state. The aggregation of citizen data from different public institutions allows governments to build a more complete view of the needs of their citizens and address what otherwise might be a disjointed experience if a citizen had to interact with multiple parties. Citizens

may view such an approach negatively, as indicative of a "surveillance state", even if the intentions are noble. Therefore, the discussion about data and trust, explored in detail in Chapter 4, is essential in ensuring that where DDPS activities are driven by the personal data of citizens, the necessary steps are taken to ensure it protects, and enhances, the trustworthiness of government.

A more visible release of public value from a DDPS approach to the "delivery" of services is in the experience of citizens crossing borders. Data exchange between countries can facilitate new forms of international co-operation such as that seen in the European Union's development of the eIDAS standard and the Mi Argentina mobile application making it possible for digital credentials to be recognised in multiple countries (Box 3.9). There are also further automated benefits, such as that between Estonia and Finland, where exchange of basic business register data is expected to facilitate the development of business between the two countries (OECD, 2015[52]).

Box 3.9. Cross-border recognition of credentials

Argentina's driving licence

In Argentina, the Mi Argentina mobile application allows citizens to access a digital version of their driving licence. It has the same legal validity as the physical equivalent and is automatically generated if the citizen is already in possession of a valid driving licence. The National Digital Driver's Licence is built on top of the Argentinian Digital Identity System that provides remote validation of citizens' identity using biometric data.

Because so many Argentinians regularly travel across the border to neighbouring Chile and Uruguay, efforts have been made with their respective governments for this digital licence to have the same validity in those countries. This approach has benefitted from the Digital Agenda Group of the Southern Common Market working together to identify and prioritise public services that could be delivered across borders.

European Regulation 910/2014 (eIDAS)

In the European Union, cross-border recognition and legitimisation of identity mechanisms are backed not by the reuse of a particular set of credentials, as in the case of Argentina, but by a focus on developing an agreed standards approach to those technical solutions.

The eIDAS regulation provides an important legal basis to the delivery of cross-border services and the easy movement of citizens from one jurisdiction to another within the single market. Established in EU Regulation No. 910/2014 of 23 July 2014, it has been providing the legal underpinnings to the conditions under which member states have developed and enhanced Digital Identity solutions that could be recognised by other countries and reused by citizens to access services throughout the single market.

From 29 September 2018, any organisation delivering public services in an EU member state must recognise electronic identification from all EU member states. The development of digital identity approaches on the basis of standards makes it possible for services to be accessed across a region without people needing to create them every time.

Sources: Jueguen, F. (2019[53]), "Lanzan la versión digital del registro de conducir que se podrá 'llevar' en el celular", https://www.lanacion.com.ar/economia/lanzan-version-digital-del-registro-conducir-se-nid2219177; Bracken, M. (2019[54]), "Argentina just made driving licences digital", https://public.digital/2019/02/12/argentina-just-made-driving-licences-digital; OECD (2019[55]), *Digital Government Review of Argentina: Accelerating the Digitalisation of the Public Sector*, https://doi.org/10.1787/24131962; European Union (n.d.[56]), *eIDAS: The Ecosystem*, https://www.eid.as/home.

Moreover, an understanding of demand for services themselves can provide a clearer view of the service delivery landscape in a society, allowing to better target specific channels to specific segments of the population to ensure no citizens are left behind. Box 3.10 provides examples from **Portugal** and **Mexico**.

Box 3.10. Using data to prioritise support for vulnerable citizens

Data analysis and an interoperability platform unlocked support for an extra 600 000 people in Portugal

In Portugal, the insights from data have transformed the support provided to some of the most vulnerable households in the country. The government created a Social Energy Tariff to subsidise energy costs. The service required eligible users to sign up and register, but the initial data showed that those who should have benefited from the tariff were not registering for it.

When research was carried out to understand why, they learnt that it was because citizens did not know that they had to ask for the special tariff. As a result, the decision was taken to automate the process. However, in order to do this, data needed to be shared between the Directorate General for Energy and Geology, energy companies, the tax system, and the social security system.

Fortunately, Portugal's Interoperability Platform for the Public Administration (iAP) had been developed for exactly this scenario, providing access to a diverse set of services from both public and private sector partners. As a direct result of being able to use the Interoperability Platform for automating the Social Energy Tariff, the number of households receiving the tariff increased from 154 648 to 726 795, providing financial support to 7% of the Portuguese population for the cost of their energy without requiring them to validate their eligibility.

Combining data to ensure support reaches those with the greatest need

In Mexico, the Ministry of Social Development is responsible for providing social services to citizens. By combining household, beneficiary and geographic data, it has been possible to build a new system for targeting support to those that need it the most with the purpose of improving the living conditions for the poorest populations in Mexico.

Working with a civil society partner, Data Science for Social Good, the Ministry of Social Development focused on increasing the accuracy of targeting the support to eligible individuals and families. The three goals were:

1. identify individuals who qualified for, but had not used, particular programmes
2. combine datasets to better predict household needs and potentially inform the design of new social service programmes
3. detect people who had under-reported their income and stop them from receiving any further assistance.

Sources: Information provided by Portugal to the OECD; Data Science for Social Good (n.d.[57]), *Enhancing the Distribution of Social Services in Mexico*, https://dssg.uchicago.edu/project/enhancing-the-distribution-of-social-services-in-mexico.

Several of the countries that participated in the comparative project that provided the baseline of insights and evidence used to back up the analysis included in this report indicated that there was an overlap in their use of data to improve public service delivery and its use in developing evidence-based policy making. This close relationship between policy design and service delivery demonstrates the importance of recognising the relationships between each phase in the application of data.

In **Denmark**, **Korea** and **Portugal**, legislation has been passed to address the needs and structure of base data registries. These are a valuable enabler for the delivery of data-driven services because they limit the proliferation of duplicate data, provide a reliable source for the most important datasets, and reflect a coherent approach to the internal access to, and sharing of, data. In **Korea**, the "Public sector big data analysis projects" have been successfully scaled to bring benefits to different population groups. These have included citizen-visible services, such as understanding where best to locate electric vehicle charging

infrastructure, through to the less public applications of data in delivery, like detecting suspected evasion of military service or tackling traffic accident-related insurance fraud.

Giving public servants the capacity to focus on meeting other needs

Improving the "delivery" of public services offers a very tangible indicator of an increase in public value from the perspective of citizens and businesses whose lives may be simplified. However, alongside those benefits are those more hidden from view in terms of their implications for internal staff.

One of the arguments that has been used to justify the digital transformation of government has been the opportunity to reduce the headcount of those working in frontline roles. As more and more services are available on line, the demand in person is expected to decrease and those roles will become redundant. This perspective is based on some incorrect assumptions. First, it expects a behaviour we cannot be certain of, i.e. that all users will shift to online platforms to access the services. Second, it takes for granted that the digital transformation is simply a quicker way of carrying out the same activities as before, rather than an opportunity to rethink the way in which services are provided. Thus, in a situation where services are transformed, the role of back office and frontline staff changes too. This can happen in several ways:

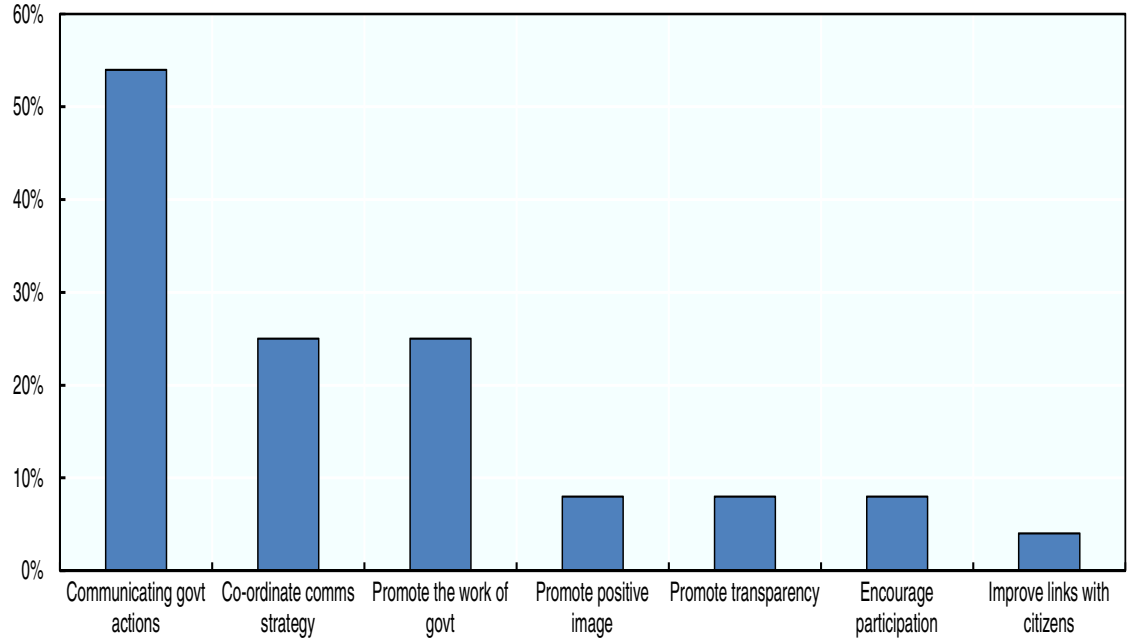
- By addressing the common case interactions, public servants are able to focus more time and energy on answering more challenging questions.
- As those who are comfortable with using digital services make the transition away from face to face services, those who continue to provide in-person support are able to devote more energy to the needs of those who might otherwise be digitally excluded.
- The increase of digital submissions and the reuse of data from across government reduces the potential for errors. This reduces the prospect of having to follow up and clarify something that can delay the fulfilment of the original service.

There are also possibilities for real-time analytical information to be used across service centres and telephone support lines to predict demand and manage staff time accordingly. For example, this could extend to developing the capability for reallocating public servants from one category of enquiry to another in response to unforeseen spikes in demand.

Communication and engagement with the public

The most recent Survey on the Organisation and Functions of the Centre of Government (OECD, 2017[58]) identified the most important objective of communication strategies. Figure 3.6 shows that communicating government actions was the highest priority, with only 8% of respondents having the objective of encouraging participation or promoting transparency, and a mere 4% reporting that they were attempting to improve links with citizens. This does not reflect the OECD *Recommendation of the Council on Open Government*, which calls for a "culture of governance that promotes the principles of transparency, integrity, accountability and stakeholder participation in support of democracy and inclusive growth" (OECD, 2017[59]). It also contrasts markedly with the strong characteristic of the OGD and open government movements where data are understood as a valuable device for fostering civic engagement in the design and delivery of public services and policies in order to strengthen a more people-driven and participatory form of democracy (OECD, 2018[26]; Ubaldi, 2013[4]).

Figure 3.6. Main objectives of the centre of government communication strategies



Source: OECD (2017[58]), *Survey on the Organisation and Functions of the Centre of Government*.

The potential for OGD to stimulate greater engagement and opportunities to communicate with the public is clear. In **Chile**, the Ministry General Secretariat of the Presidency put out a call to artists to develop original digital content with OGD and showcase the possibilities. In every corner of the globe, countries are hosting hackathons that encourage teams to come together and work with OGD in response to particular challenges; these include the Accountability Hackathon in the **Netherlands**, the CANDEV data challenge in **Canada**, the OpenGovDataHack and Hack the Plan in **India**, and GovHack in **Australia**, among others.

However, the experience of **Sweden** and HackforSweden (OECD, 2019[60]) is particularly inspirational. HackforSweden currently works with almost 100 Swedish government agencies and companies to promote innovation through open data with the explicit intent to create a platform for citizen-driven responses to societal needs and seeking collaboration to co-create public value. From humble beginnings in 2014, HackforSweden is now moving away from annual events to seek ongoing engagement and creativity from the digital ecosystem in the country with the mission to swap 200 people at an event for 2 million people connected through a platform in just 2 years (Hack for Sweden, n.d.[61]).

Outside of OGD, the potential for DDPS approaches to be utilised by governments to communicate with the public is currently underexploited. According to the comparative research carried out with the six OECD countries, only **Denmark** and **Sweden** could provide concrete examples of how policy initiatives were in place to encourage the use of data to engage societal stakeholders. This means that **Korea**, **Ireland**, **Portugal** and the **United Kingdom** have not made this a priority.

This is unfortunate because the use of data can support the process of debating policy options with visualisations offering accessible ways of presenting detailed information about particular problems. Concepts that are hard to communicate verbally or dense sets of numbers or co-ordinates can be transformed into tools that facilitate valuable discussion and engagement exercises. In the context of generating public value, Morabito (2015[62]) argues that communicating how data have been used in accessible ways can have a positive effect on citizens' sense of achievement and their satisfaction with government services.

In **Denmark**, the approach to property tax was redesigned in order to provide citizens with a more transparent view of the system based on better data and the use of improved statistical methods. In handling the transition from old to new, data visualisations were used to provide clarity for citizens. By prioritising transparency and openness in the change, citizens were not only able to understand the policy in general terms, but the government invested in the capabilities and data literacy of citizens to understand how it affected them specifically.

Responding to emergencies, crises and developing situations

The final area of opportunity for adding public value associated with the "delivery" phase of the DDPS is the way in which public sector organisations are able to respond to emergencies, crises and developing situations.

Emergencies and crises by their very nature cannot be predicted. While their impacts can be minimised, it is impossible to be prepared for every eventuality at all times. This underscores the importance of the "anticipation and planning" stages in terms of the design and foresight activities for thinking through what might be needed in the event something went wrong. Indeed, the OECD *Recommendation of the Council on the Governance of Critical Risks* emphasises the importance of building preparedness through foresight analysis, risk assessments and financing frameworks, to better anticipate complex and wide-ranging impacts (OECD, 2014[63]).

In Seoul, **Korea,** the mayor has invested a significant amount of money in developing a 3.5 metre wide dashboard on the wall of the office providing a real-time feed of interesting data about the health and vitality of the city and its inhabitants, including the cost of living, demand for housing and the real-time budget position. This is helpful operational insight that can shape the political priorities and ongoing service delivery in the city. However, the effort has been made to consider how this resource might add value in the event of an emergency. During an emergency, the dashboard comes into its own, providing a live feed of the situation unfolding and giving the mayor direct contact with those on the ground (Crawford, 2017[64]).

In **Singapore**, the challenges of overcrowded and ageing transport infrastructure coupled with the country's "smart nation" ambitions prompted the development of the Fusion Analytics for Public Transport Emergency Response (FASTER) initiative. With FASTER, anonymised location-based information is collected and combined with fare card transactions and video feeds from stations to identify overcrowding. When crowds are detected, additional buses are deployed and messages are relayed to customers allowing them to plan accordingly. These data provide detailed models of how users move through the city, helping the government to understand traffic patterns, how the transport network is used and issues to address with the network.

Evaluation and monitoring

The third and final set of behaviours in the DDPS framework for applying data to generate public value is that of "evaluation and monitoring". A DDPS recognises that ongoing evaluation and monitoring is enhanced through the application of relevant data. These activities focus on measuring and analysing activity that has already happened. While a reaction to this may take place in the short term, the purpose of this activity may also stand alone as a reflection on what has been achieved or grow in value after some time when it is used to inform a new purpose.

The evaluation of performance and monitoring of a real-time data society is closely tied to the "delivery" activities discussed in the previous section. The data generated in this phase inform the "anticipation and planning" of subsequent projects. This phase is critical in shaping the pace of decision making, targeting of investment and capacity to respond to change. Crucially, the perspective in this section is that data in the public sector lead to an understanding of performance, so that an iterative approach to either the

ongoing refinement of activity or subsequent planning follows. This is not simply reporting for the sake of reporting.

A DDPS fosters an environment in which data about real-time policy interventions are available. Policy makers no longer have to wait for monthly or quarterly updates in areas such as migration, unemployment and demographics, because the data they need are becoming available, and accessible, at a higher frequency. Consequently, this provides better insights into the policy process and enables quick policy adjustments in the short term, resulting in increased accountability and continuous improvement in the mid- and long terms.

This highlights the interconnectedness between the different dimensions of the DDPS value framework and underscores how important it is that no "anticipation and planning" or "delivery" should take place without considering the question of how activity will be evaluated, performance monitored and impact measured. In light of that, this section will consider policy evaluation, operational performance, demonstrating return on investment, and accountability and transparency. The kind of data activities that will be discussed are those which look to allow the measurement of impact, the auditing of decisions and the monitoring of performance.

Policy evaluation

The first area in which the "evaluation and monitoring" of data can generate public value is in the process of evaluating the success, or otherwise, of policy interventions. In a well-functioning democratic society, the implementation of policy is scrutinised by a variety of actors. There are those who wish to ensure government resources have been effectively managed, those motivated by a desire to understand the impact of the intervention and those who may be looking for political opportunity to exploit. These actors have competing priorities, but the reporting of progress, particularly if done in public, offers an evidence-generating activity that can hold the tension of the spectrum between politically motivated and ideological claims at one end, and theoretically unbiased and rational evidence-based policy making at the other.

In this sense, the evaluation of policy after its implementation complements the use of evidence in the initial design and development of a policy intervention. The insights generated from evaluating policy are critical for iterating and developing new policy approaches and it is in responding to the evaluation of what has been done that governments can generate public value. Nevertheless, beyond the direct application of data in shaping government activity, "evaluation and monitoring" data serve an important role when shared in being used, and reused, to inform and equip politicians, journalists, academics and the wider public.

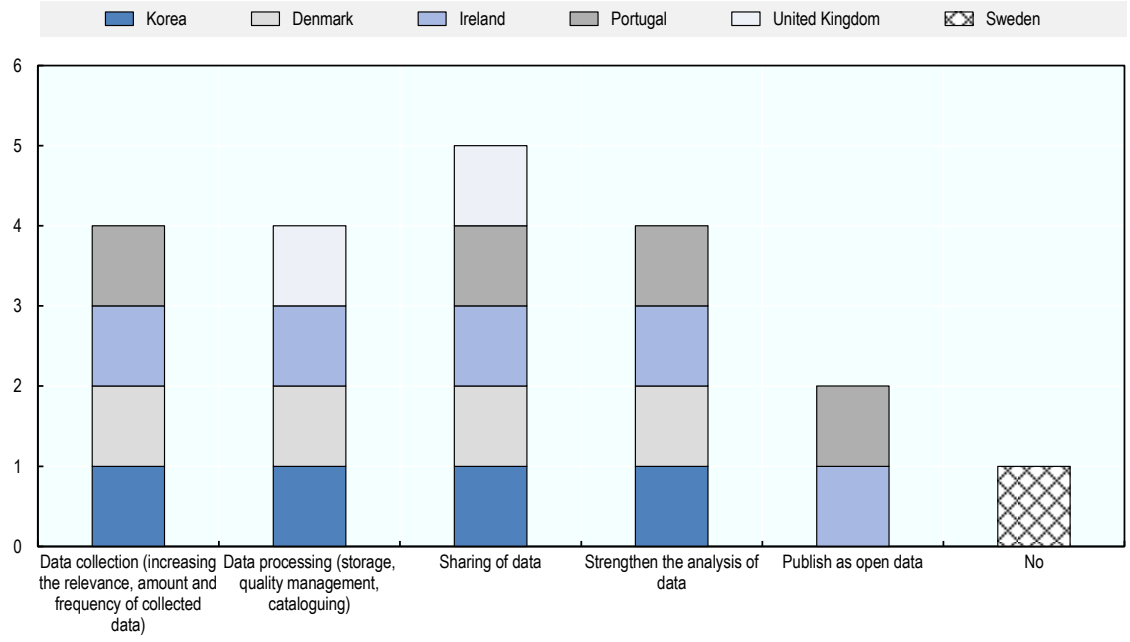
Increasing the amount of data associated with the outcome of a given policy allows for agile policy adjustments in the short term, but more importantly will generate better insights into the policy process in terms of accountability and learning in the mid- to long term. Those responsible for a given policy can establish whether their policies have had the desired effect or not and, if those data are published as OGD, so can other stakeholders. As a result, policy evaluation can turn into an open, inclusive and ongoing process rather than an internal, snapshot moment. The ability to reduce the lag between the design of a policy, its implementation and insights into its performance should not just have theoretical and conceptual value, but should provide the basis for rapidly informing "delivery" activity and remedying any unintended adverse effects (Höchtl, Parycek and Schöllhammer, 2016[47]). While the monitoring of performance might be prompted by a top-down desire for oversight and reporting on delivery, a DDPS is interested in how those insights can be analysed and, crucially, applied in improving performance based on a deeper understanding of the needs of the organisation and its users.

Carrying out retrospective evaluation and analysis is helpful in keeping an open mind as it encourages an ongoing learning from experience and stimulates efforts to adapt future policy as a result. Putting in place mechanisms to gather, and apply, new insights set an expectation that lessons will be learnt and new

insights gained. Taking this approach enhances the ongoing quality of outcomes. The OECD/Bloomberg (2019[49]) report on *Enhancing Innovation Capacity in Cities* establishes that "those cities which evaluate … are better positioned to scale up innovative projects that improve operations, and less likely to engage in practices or projects that offer little return on investment". Being open to the "evaluation and measurement" of impact is indicative of a more sophisticated appreciation for the role of data that will manifest itself throughout the policy and delivery life cycle.

It is therefore encouraging that Figure 3.7 shows five of the six researched countries (**Korea**, **Denmark**, **Ireland**, **Portugal** and the **United Kingdom**) implementing some steps to strengthen policy monitoring and evaluation throughout the government data value cycle. **Denmark**, **Ireland**, **Korea** and **Portugal** are particularly focused on how they might strengthen policy monitoring and evaluation by investing in the capacity to analyse the data. As discussed in Chapter 2 in the context of identifying the necessary conditions for successfully implementing the DDPS, the skills of public servants, and the public, are critical for maximising public value. All five of those countries have taken steps to make the sharing of data a focus, which as discussed at the beginning of this chapter is a critical factor in successfully creating a whole-of-government approach to generating public value through data.

Figure 3.7. In what areas has your country implemented policy initiatives to strengthen policy monitoring and evaluation through better data management and use?



Source: Based on information provided by six OECD countries in response to the Questionnaire on the State of the Data-driven Public Sector in OECD Countries, Question 16: "Has your country implemented policy initiatives at the central/federal level to strengthen policy monitoring and evaluation through better data management and use? (e.g. using data to enable continuous and/or automated policy monitoring and inform agile policy adjustments)".

The previous section discussed the role of data in enhancing communication and engagement between the public sector and the public. Those examples discussed how the government to citizen relationship might be facilitated, but there are opportunities and possibilities for government to develop a greater understanding of the impact of policy on citizens. In a DDPS, organisations can analyse a wealth of input to evaluate policies from crowdsourcing initiatives, but they may also be able to gather these insights without necessarily asking for them directly, as discussed in Box 3.11. Similar to some of the practices mentioned in the earlier discussion on forecasting, data from a myriad of digital channels can be accessed

and analysed, revealing the opinions and behaviours of citizens, and subsequently used to evaluate policy. When exploring these issues, governments must act with sensitivity and in ways that are informed by the framing of the debate in Chapter 4.

Box 3.11. Tunisia: Using social media to track progress on the Sustainable Development Goals

To monitor progress with Sustainable Development Goal (SDG) 16 on Peace, Justice and Strong Institutions, which has a key focus on corruption, the Tunisian National Statistics Institute and the United Nations Development Programme launched a pilot using social media to better understand citizens' perceptions of government. Traditional methods (such as household surveys) were insufficient because of their infrequency and cost.

The pilot involved conducting a network analysis of web and social media (e.g. news, blogs and Twitter) to identify relevant content and determine whether its tone was positive or negative in order to gauge citizen perceptions of corruption. To help determine accuracy, the team compared the results of the social media analysis with the results of Tunisia's Household Survey on Governance, Peace and Democracy, which contained questions on citizen perceptions of corruption. Over the same time frame, both the survey and social media provided the same perception on corruption, and the social media analysis had the additional benefit of being faster, more regular and less expensive. Tunisia has begun testing this approach with other targets from the same SDG, namely human rights and rule of law, and civic participation.

Source: OECD (2017[65]), *Fostering Innovation in the Public Sector*, https://dx.doi.org/10.1787/9789264270879-en.

Operational performance

A second area for considering the "evaluation and monitoring" activity of the DDPS is in how data can transform the operational performance of government, leading to both more productive and effective use of public resources and developing a culture of continuous performance improvement. Measuring performance is an "evaluation and monitoring" activity that has to happen retrospectively. Nevertheless, applying its insights, it is tightly coupled with the quality of government "delivery". This relationship once again highlights how important it is for clarity about the purpose behind the application of any data.

Public value can be unlocked in terms of the direct impact it has on the activity of government, as discussed in the "delivery" section, but also in the more hidden, structural activities of government. For example, data about the real-time status of physical assets can be used to better plan maintenance with the least disturbance to service continuity as possible (OECD, 2016[66]). The complementary case study "Data-Driven Human Resource Management" focusing on public employment and management highlights how people analytics might change approaches to recruitment, retention and the ongoing performance management of staff, as well as understanding how to improve the environment in which they work to ensure their productivity and well-being.

While an increasing amount of our transactional relationships are moving on line, safeguarding the built environment and our material conditions continues to be an important function of government. The application of data can allow for targeting scarce resources, such as focusing policing on areas with high criminal activity (Höchtl, Parycek and Schöllhammer, 2016[47]).

In **Korea** and **Portugal**, entrants to competitions focused on the use of data have been encouraged to target improvements to the efficiency of government operations. One of the success stories from **Korea** is the development of a data model for identifying businesses most likely to present a risk. Twelve months after its introduction, there had been an increase in the proportion of inspected workplaces violating the Labour Standards Act from 40.9% to 77.7%, almost doubling the impact of inspection staff in terms of

public value. A similar impact was achieved in the **United States,** where the city of New York's Department of Buildings pooled data with 19 other city agencies. The outcome of that collaboration was a five-fold return on the value of an inspector's time, with the rate of detecting high-risk property conditions increasing from 13% of inspections to above 70% (OECD, 2018[26]).

Demonstrating return on investment

Because public sector organisations are accountable for the money they spend and there are always more demands for funding than there are available resources, sophisticated investment and procurement processes have been developed. The OECD *Recommendation of the Council on Public Procurement* (2015[67]) promotes a strategic approach throughout the different sectors and levels of the public sector with guiding principles addressing the entire procurement life cycle. Specifically within the context of digital government, Recommendation 9 of the OECD *Recommendation of the Council on Digital Government Strategies* (2014[68]) emphasises the importance of business cases to reinforce digital policy. The ongoing work of the OECD Working Party of Senior Digital Government Officials (E-Leaders) has included a focus on developing business cases and transforming ICT commissioning.

This third aspect of "evaluation and monitoring" looks at the way in which a DDPS approach can support arguments for funding and measurement of the impact of that spend. Public value in this case is then much more closely aligned with financial accountability over spend, improved procurement decisions and the ability to describe the outcomes that were made possible. In **Denmark**, several initiatives within the national digitisation strategy are informed and supported by an analysis of the value of data sharing in the transformation of internal activities within government.

Demonstrating return on investment is another activity that relies strongly on the clarity of intent for any DDPS activity. Measuring the impact of a given set of activities requires setting a baseline and developing a methodology to understand costs and benefits. These need to be considered when a public sector organisation is deciding to invest money in tackling a problem or designing a policy intervention during the "anticipation and planning" stage. They then need to have been implemented during the "delivery" phase. This ensures that there is always recognition of the value of an investment, as the example in Box 3.12 shows.

In the context of data-related spending, and particularly OGD, the focus has sometimes been on measuring the act of publication as a policy outcome, resulting in the objective to increase the number of datasets available for public access. This can mean efforts are made to releasing data rather than for its reuse. While release is a prerequisite for creating value in the use of data, any measurement for calculating the public value returned through investment on data-related efforts needs to consider defining benchmarks for both the sharing, curating and publishing stage and the use and reuse stage of the government data value cycle.

Box 3.12. Compliance with Her Majesty's Revenue and Customs in the United Kingdom

The United Kingdom's HM Revenue and Customs department has developed data models to help focus its compliance activities. The models help to identify people who may be most likely to be non-compliant on their taxes, such as by making errors in their tax returns or deliberately trying to evade taxes. The models take into account information such as taxpayers' prior compliance and information from the tax return itself, such as income and occupation, in order to assign a risk probability of non-compliance. A wide range of data can be fed into these models to assist in calculating the risk probabilities, and as the amount of data grows, so does the ability to build on the models to improve their performance.

Oversight programmes such as this offer some of the easiest ways to earn returns on investment for government analytics projects, as the financial savings are often significant. The analytics model for targeting value-added tax evasion is estimated to bring in around GBP 200 million a year in additional revenue due to improved compliance-targeting efforts, doubling the amount of revenue collected for each compliance caseworker.

Source: OECD (2017[65]), *Fostering Innovation in the Public Sector*, https://dx.doi.org/10.1787/9789264270879-en.

Accountability through audit trails and transparency

This final area of the "evaluation and monitoring" activity within the DDPS concerns accountability, and in particular the role of data as a tool for providing access to government records and encouraging a culture of transparency. The role of integrity actors in government relies heavily on the successful implementation of the DDPS. The case study on "Data-Driven Integrity" highlights the opportunities that present themselves in an associated but different approach to accountability, namely the prevention of fraud and corruption.

The importance of auditing activities and the desire for transparency in government should not be underestimated as the basis for making the argument about increasing the profile of data-related activity within government. In the context of OGD, that agenda has been a significant driver in seeing data published in line with the OECD *Recommendation of the Council on Open Government* (OECD, 2017[59]; Ubaldi, 2013[4]).

More broadly, public sector organisations should be interested in exploring how the impact of a policy can be demonstrated in ways that build accountability and stimulate trust with the public. This echoes some of the discussion earlier in the chapter around the analysis of "delivery" activities. Box 3.13 presents the example of **Japan**, whose whole-of-government approach to evidencing the impact of policy comes from the very top of the government (supporting the importance of leadership and vision discussed in Chapter 2). Within that context, the analysis and evaluation of a policy intervention is not only seen as promoting greater accountability, but provides the underpinning to ensure that a particular policy intervention is having the desired effect. Adopting robust methods like these to measure, and publish, the evidence about the reality of a policy or service not only during a pilot or alpha but throughout, can form the basis of arguing for future funding and, over time, demonstrate return on investment as well as helping to create a culture of accountability.

Box 3.13. Using evidence to evaluate the effectiveness of policy interventions in Japan

Data governance

In Japan the Strategic Conference for the Advancement of Public and Private Data Utilization, chaired by the Prime Minister and comprising all ministers, government chief information officers and expert advisors, has had national oversight for the data agenda since 2017. Support is provided by the Council on Promoting Evidence-based Policymaking and the presence of a Director-General for Evidence-based Policymaking in each ministry.

During the policy life cycle, the Administrative Evaluation Bureau within the Ministry of Internal Affairs and Communications and the Administrative Reform Promotion Headquarters Secretariat assess every policy evaluation and project review to check that evidence and data are being used at every stage. The data in these reviews are openly available to the public and the process can be watched on line.

This accountability is not only valuable for increasing democratic governance, reliability, integrity and legitimacy, but also ensures there is a continuous empirical challenge to whether or not a policy intervention is achieving the intent that was originally envisioned.

Using randomised controlled trials to evaluate Internet of Things technologies

Japan's ageing population means that it is a priority to identify ways in which technology can contribute to the provision of high-quality and effective care while reducing costs. One area of focus has been on the care for patients suffering from dementia and exploring whether Internet of Things (IoT) devices could help prevent the disease or reduce the costs associated with its treatment.

In the first case, dementia patients accommodated in nursing facilities were randomly divided into two groups. One group acted as the control group and had no change to their care while the other group underwent interventions using IoT services. The symptoms of dementia disappeared within four months for 34% of the control group and 74% of the intervention group.

In the second case, IoT devices were provided to patients and their activity logged and scored. Based on the data supplied to their medical teams, patients were rewarded with points. Those points could be used like cash. A baseline for healthcare costs was established for each of those who received the devices and those who formed part of the control. After a year, the increase in healthcare costs from that baseline was calculated. The data showed that on average the healthcare costs of those using IoT devices were 56% of those in the control group, a saving per patient of JPY 50 000. Among the most elderly patients, the saving was JPY 90 000.

Source: Advisor to the Ministry of Internal Affairs and Communications, Japan (2019), "Is evidence contributing to public accountability? Evidence from Japan".

In **Portugal**, the Health Service Transparency Portal,[3] and the justice transparency portal[4] provide open access to performance data on a sectoral basis. Moreover, at the municipal level, data and dashboards are provided by the Municipal Transparency Portal,[5] detailing the local use of public money and the performance of the services they provide. In **Denmark**, Statistics Denmark[6] provides a common platform for reporting data relating to the performance of the country. These performance insights include the presentation of data about the effectiveness of policy. In the **United Kingdom**, all services are required to publish their performance data as part of the Service Standard, but this does not always identify the success, or otherwise, of a service in relation to its policy intent.

References

Acquah, D., K. Lisek and S. Jacobzone (2019), "The role of evidence informed policy making in delivering on performance: Social investment in New Zealand", *OECD Journal on Budgeting*, No. 19, OECD Publishing, Paris, https://dx.doi.org/10.1787/74fa8447-en. [39]

Arnold, T. (2014), "Inside the Convention on the Constitution", *The Irish Times*, https://www.irishtimes.com/news/politics/inside-the-convention-on-the-constitution-1.1744924. [41]

ASEDIE (2019), *2019 Infomediary Sector*, Asociación Multisectorial de la Información, http://www.asedie.es/assets/asedie.-infomediary-sector-report-2019.pdf. [25]

Bracken, M. (2019), "Argentina just made driving licences digital", *Public Digital*, https://public.digital/2019/02/12/argentina-just-made-driving-licences-digital. [54]

Breckon, J., A. Hopkins and B. Rickey (2019), *Evidence vs Democracy: How "Mini-publics" Can Traverse the Gap Between Citizens, Experts, and Evidence*, Alliance for Useful Evidence, https://media.nesta.org.uk/documents/Evidence_vs_Democracy_Report_Final.pdf. [40]

Cabinet Office et al. (2013), *Applying Behavioural Insights to Organ Donation: Preliminary Results from a Randomised Controlled Trial*, Cabinet Office, London, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/267100/Applying_Behavioural_Insights_to_Organ_Donation.pdf. [50]

ConsultingWhere Limited and ACIL Tasman (2013), *Assessing the Value of OS OpenData™ to the Economy of Great Britain - Synopsis*, Department for Business, Innovation & Skills, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/207692/bis-13-950-assessing-value-of-opendata-to-economy-of-great-britain.pdf (accessed on 1 July 2019). [28]

Crawford, S. (2017), *How South Korea is Building a Techno-Utopia in Seoul*, https://www.wired.com/story/how-seoul-is-reinventing-itself-as-a-techno-utopia (accessed on 15 November 2018). [64]

Cresswell, A., G. Burke and T. Pardo (2006), *Advancing Return on Investment Analysis for Government IT: A Public Value Framework*, Center for Technology in Government, University at Albany State University of New York, https://www.ctg.albany.edu/media/pubs/pdfs/advancing_roi.pdf. [35]

Data Science for Social Good (n.d.), *Enhancing the Distribution of Social Services in Mexico*, https://dssg.uchicago.edu/project/enhancing-the-distribution-of-social-services-in-mexico. [57]

Deloitte (2016), *Global Human Capital Trends 2016*, Deloitte, http://www.deloitte.com/us/hctrends (accessed on 14 February 2019). [48]

Department of the Navy (2017), *Strategy for Data and Analytics Optimization*, US Department of the Navy, https://www.doncio.navy.mil/uploads/Final_DON%20Strategy%20for%20Data%20and%20Analytics%20Optimization.pdf. [2]

Dods, S. et al. (2013), *Evidence-Driven Strategies for Meeting Hospital Performance Targets: The Value of Patient Flow Modelling*, CSIRO, https://doi.org/10.4225/08/584c43f4df82b. [46]

European Union (n.d.), *eIDAS: The Ecosystem*, https://www.eid.as/home (accessed on 29 August 2018). [56]

Finansdepartementet S3 (1998), *Förordning (1998:1234) om det statliga personadressregistret*, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-19981234-om-det-statliga_sfs-1998-1234 (accessed on 26 July 2019). [9]

Geovation (2019), *Geovation website*, https://geovation.uk (accessed on 4 July 2019). [43]

Godfrey, J. et al. (2010), *Accounting Theory*, John Wiley, https://www.wiley.com/en-au/Accounting+Theory,+7th+Edition-p-9780470818152. [13]

Government of Korea (2017), *Electronic Government Act*, http://www.law.go.kr/LSW/eng/engLsSc.do?menuId=1&query=%EC%A0%84%EC%9E%90%EC%A0%95%EB%B6%80%EB%B2%95&x=0&y=0#liBgcolor0. [7]

Hack for Sweden (n.d.), *The Mission*, https://hackforsweden.se/the-mission (accessed on 12 July 2019). [61]

Henderson, S. et al. (2017), *Issues in Financial Accounting, 16th Edition*, Pearson, https://pearson.com.au/products/H-J-Henderson-Scott-et-al/O-R-Peirson-Henderson-Herbohn-Artiach-How/Issues-in-Financial-Accounting/9781488611643?R=9781488611643. [14]

Hickling Arthurs Low Corporation (2015), *Canadian Geomatics Environmental Scan and Value Study*, Natural Resources Canada, http://giscourses.net/wp-content/uploads/2015/05/Canadian-Geomatics-Environmental-Scan-and-Value-Study.pdf?189db0. [29]

HM Treasury (2019), *Public Value Framework*, HM Treasury, London, https://www.gov.uk/government/publications/public-value-framework-and-supplementary-guidance. [36]

HM Treasury (2018), *The Green Book: Central Government Guidance on Appraisal and Evaluation 2018*, HM Treasury, London, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/685903/The_Green_Book.pdf. [37]

Höchtl, J., P. Parycek and R. Schöllhammer (2016), "Big data in the policy cycle: Policy decision making in the digital era", *Journal of Organizational Computing and Electronic Commerce*, Vol. 26/1-2, pp. 147-169, http://dx.doi.org/10.1080/10919392.2015.1125187. [47]

Indeed Hiring Lab (2019), *Data Scientist: A Hot Job That Pays Well*, Indeed Hiring Lab, https://www.hiringlab.org/2019/01/17/data-scientist-job-outlook. [12]

Jueguen, F. (2019), "Lanzan la versión digital del registro de conducir que se podrá 'llevar' en el celular", *La Nacion*, https://www.lanacion.com.ar/economia/lanzan-version-digital-del-registro-conducir-se-nid2219177 (accessed on 29 March 2019). [53]

Ladley, J. (2010), *Making Enterprise Information Management (EIM) Work for Business: A Guide to Understanding Information as an Asset*, Morgan Kaufmann, https://doi.org/10.1016/C2009-0-61376-3. [17]

Laney, D. (2017), *Infonomics: How to Monetize, Manage, and Measure Information as an Asset for Competitive Advantage*, Routledge, New York, NY, http://dx.doi.org/10.4324/9781315108650. [18]

Local Government Denmark (2012), *Good Basic Data for Everyone: A Driver for Growth and Efficiency*, Local Government Denmark, https://en.digst.dk/media/18773/good-basic-data-for-everyone-a-driver-for-growth-and-efficiency.pdf. [11]

Lund, S. et al. (2013), *Game Changers: Five Opportunities for US Growth and Renewal*, McKinsey & Company, https://www.mckinsey.com/featured-insights/americas/us-game-changers (accessed on 14 February 2019). [33]

Manyika, J. et al. (2011), *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, McKinsey & Company, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation (accessed on 14 February 2019). [32]

McAfee, A. and E. Brynjolfsson (2012), *Big Data: The Management Revolution*, https://hbr.org/2012/10/big-data-the-management-revolution. [34]

Meynhardt, T. (2009), "Public value inside: What is public value creation?", *International Journal of Public Administration*, Vol. 32/3-4, pp. 192-219, http://dx.doi.org/10.1080/01900690902732632. [23]

Moody, D. and P. Walsh (1999), *Measuring the Value of Information: An Asset Valuation Approach*, European Conference on Information Systems, http://si.deis.unical.it/zumpano/2004-2005/PSI/lezione2/ValueOfInformation.pdf. [16]

Moore, M. (1997), *Creating Public Value: Strategic Management in Government*, Harvard University Press. [22]

Morabito, V. (2015), *Big Data and Analytics*, Springer International Publishing, Cham, http://dx.doi.org/10.1007/978-3-319-10665-6. [62]

Nuffield Foundation (2019), *Valuing Data: Foundations for Data Policy*, Nuffield Foundation, London, https://www.nuffieldfoundation.org/valuing-data-foundations-data-policy (accessed on 10 July 2019). [15]

OECD (2019), *Digital Government Review of Argentina: Accelerating the Digitalisation of the Public Sector*, OECD Publishing, Paris, https://doi.org/10.1787/24131962. [55]

OECD (2019), *Digital Government Review of Sweden: Towards a Data-driven Public Sector*, OECD Publishing, Paris, http://dx.doi.org/doi.org/10.1787/24131962. [19]

OECD (2019), *Digital Government Review of Sweden: Towards a Data-driven Public Sector*, OECD Publishing, Paris, https://doi.org/10.1787/4daf932b-en. [60]

OECD (2018), *Open Government Data Report: Enhancing Policy Maturity for Sustainable Impact*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264305847-en. [26]

OECD (2017), *Fostering Innovation in the Public Sector*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264270879-en. [65]

OECD (2017), *Government at a Glance 2017*, OECD Publishing, Paris, https://dx.doi.org/10.1787/gov_glance-2017-en. [27]

OECD (2017), *How's Life? 2017: Measuring Well-being*, OECD Publishing, Paris, https://dx.doi.org/10.1787/how_life-2017-en. [38]

OECD (2017), *Recommendation of the Council on Open Government*, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0438. [59]

OECD (2017), *Survey on the Organisation and Functions of the Centre of Government*, OECD, Paris. [58]

OECD (2016), *Open Government Data Review of Mexico: Data Reuse for Public Sector Impact and Innovation*, OECD Publishing, Paris, https://doi.org/10.1787/24131962. [45]

OECD (2016), "The Internet of Things: Seizing the benefits and addressing the challenges", *OECD Digital Economy Papers*, No. 252, OECD Publishing, Paris, http://dx.doi.org/10.1787/5jlwvzz8td0n-en. [66]

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264229358-en. [5]

OECD (2015), *OECD Public Governance Reviews: Estonia and Finland: Fostering Strategic Capacity across Governments and Digital Services across Borders*, OECD Public Governance Reviews, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264229334-en. [52]

OECD (2015), *OECD Recommendation of the Council on Public Procurement*, OECD, Paris, http://www.oecd.org/gov/public-procurement/recommendation. [67]

OECD (2015), *Rebooting Public Service Delivery: How Can Open Government Data Help to Drive Innovation?*, OECD, Paris, http://www.oecd.org/gov/Rebooting-Public-Service-Delivery-How-can-Open-Government-Data-help-to-drive-Innovation.pdf. [42]

OECD (2014), *Recommendation of the Council on Digital Government Strategies*, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406. [68]

OECD (2014), *Recommendation of the Council on the Governance of Critical Risks*, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0405. [63]

OECD (2010), *Denmark: Efficient e-Government for Smarter Public Service Delivery*, OECD e-Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264087118-en. [10]

OECD (forthcoming), *Standards of Evaluation: A Review of International Perspectives*, OECD, Paris, forthcoming. [44]

OECD Observatory of Public Sector Innovation (2019), "Hello, world: Artificial intelligence and its use in the public sector", draft, OECD Observatory of Public Sector Innovation, Paris, https://oecd-opsi.org/projects/ai. [20]

OECD/Bloomberg (2019), *Enhancing Innovation Capacity in Cities*, OECD Publishing, Paris. [49]

Pollock, R. (2010), *Welfare Gains from Opening Up Public Sector Information in the UK*, University of Cambridge, http://www.rufuspollock.org/economics/papers. [30]

Presidência do Conselho de Ministros (2015), *Resolution of the Council of Ministers No.42/2015*, https://dre.pt/home/-/dre/67540636/details/maximized?p_auth=7PgkXEza. [8]

Ries, E. (2011), *The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses*, Currency. [51]

Talbot, C. (2011), "Paradoxes and prospects of 'public value'", *Public Money & Management*, Vol. 31/1, pp. 27-34, http://dx.doi.org/10.1080/09540962.2011.545544. [24]

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, https://dx.doi.org/10.1787/5k46bj4f03s7-en. [4]

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. [21]

United States White House (2018), *President's Management Agenda*, United States White House, https://www.whitehouse.gov/wp-content/uploads/2018/03/Presidents-Management-Agenda.pdf. [31]

US Department of Health & Human Services (2011), *Improving Data for Decision Making: HHS Data Collection Strategies for a Transformed Health System*, US Department for Health & Human Services, Washington, DC, https://aspe.hhs.gov/basic-report/improving-data-decision-making-hhs-data-collection-strategies-transformed-health-system. [1]

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://doi.org/10.1787/09ab162c-en. [3]

Welby, B. (2019), "The impact of digital government on citizen well-being", *OECD Working Papers on Public Governance*, No. 32, OECD Publishing, Paris, https://doi.org/10.1787/24bac82f-en. [6]

Notes

[1] https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering.

[2] https://oecd-opsi.org/search-toolkits/?_sft_discipline-or-practice=futures-and-foresight.

[3] https://www.sns.gov.pt/transparencia.

[4] https://partilha.justica.gov.pt.

[5] https://www.portalmunicipal.gov.pt.

[6] https://www.dst.dk/da.

4 The role of data in building trust

This chapter starts by explaining the determinants of trust to better identify the key areas that contribute to institutional trust building. It then explores the potential of using data to build trust, including adopting ethical approaches, protecting the privacy of data, securing transparency and mitigating risks. The chapter will then provide examples of countries that have successfully implemented good practices, and concludes with a list of data ethics guidelines that could help civil servants manage the use of data in an ethical way.

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

Introduction

When countries meet all the conditions for good data governance (see Chapter 2), they set the foundations to draw insights from data to improve policy making and public service design and delivery (Chapter 3), and increase citizens' well-being. The quality of public service therefore better meets citizens' needs. Yet, this results in the need to strengthen the focus on efforts aimed at reinforcing trust in the way governments handle citizens' data.

Increasing access to data while retaining trust is a challenge for many governments. Since trust is difficult to earn and maintain, and even more challenging to restore, preserving public trust has been and always will be crucial for governments. It is therefore important not only to explore the determinants of trust (responsiveness, reliability, integrity, openness and fairness) and understand how trust can be maintained through regulations and practices on the use of data, but also to examine how it can be lost if the use of data is not carefully anticipated. This gives a better understanding of the concept of trust using data in the public sector.

This chapter addresses how governments build data trust. It discusses practical ways in which governments and citizens are collaborating on four aspects that matter for building or maintaining trust: 1) ethics; 2) privacy and consent; 3) transparency; and 4) security.

This chapter is structured as follows. First, it will explain the determinants of trust to better identify the key areas that contribute to institutional trust building. It will then explore the potential of using data to build trust, including adopting ethical approaches, protecting the privacy of data, securing transparency and mitigating risks. The chapter will then provide examples of countries that have successfully implemented good practices, and concludes with a list of data ethics guidelines that could help civil servants manage the use of data in a responsible way.

Determinants of trust

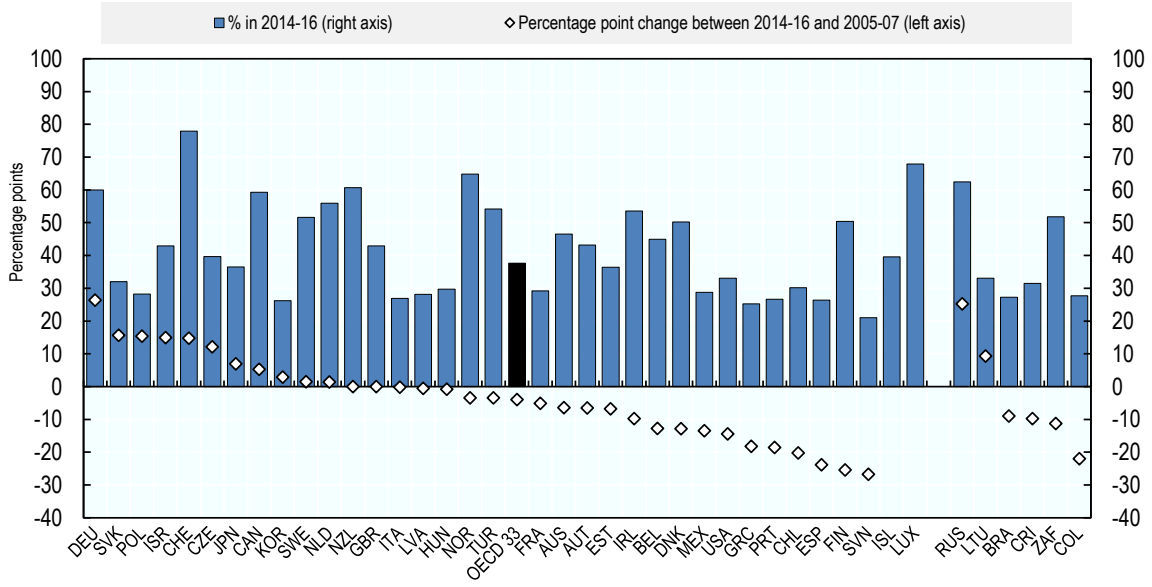
Trust has been defined in several ways by different researchers (McKnight and Chervany, 2000[1]). In this chapter, the word "trust" will refer to "a person's belief that another person or institution will act consistently with their expectations of positive behaviour", based on OECD (2017[2]).

Trust has been identified by many scholars as a dominant factor of social and economic advancement (Putman, Leonardi and Nanetti, 1993[3]; Ahn and Hemmings, 2000[4]). Both trust in an institution and trust in a person affect income per capita and the economic progress of a country, health situation and health-related behaviour, crime rates and personal well-being. Major events in the past decade, such as the government response to and preparation for natural disasters or the financial crisis of 2008, explain the decline in trust in public institutions. This decline has led to a rise of populism and a decrease in voting participation, which has been alarming in many OECD countries (Murtin et al., 2018[5]).

Data show that from 2005-07 to 2014-16, people's trust in their government decreased on average by four points in OECD countries (Figure 4.1). Only 38% of participants reported having confidence in their national government (OECD, 2017[6]).

To study this phenomenon, the OECD conducted research on the determinants of trust and developed a framework that examines trust under three angles: individual, institutional and societal. At an institutional level, people are engaged to establish collaboration and build trust in institutions themselves. Findings show that people look at government competences to deliver services and government values they promote when taking decisions and whether to trust an institution (OECD/KDI, 2018[7]).

Figure 4.1. Average confidence in national government in the period 2014-16, and the change in respect to the period 2005-07



Note: The OECD average is population-weighed and excludes Iceland and Luxembourg due to incomplete data.
Source: OECD calculations based on Gallup World Poll, www.gallup.com/services/170945/world-poll.aspx.

Government competences include two dimensions: 1) responsiveness, which is the effectiveness of meeting people's needs and expectations while gradually changing over time in order to meet demand; and 2) reliability, which is the ability to reduce and manage social, economic and political uncertainty in an effective manner. Citizens are more likely to trust institutions that manage to provide tailored quality public services, since research shows that institutional trust was highly linked to people's satisfaction with public services (Murtin et al., 2018[5]). This correlation is especially stronger at the local level than at the central level, as local governments interact more frequently with citizens, thus they are more likely to produce better solutions and maintain the public's confidence (OECD, 2017[8]). This confirms the idea that better customer services lead to stronger trust (Aberbach, 2007[9]).

Government values encompass three dimensions: 1) integrity, which means low corruption within the system and high standards of accountability; 2) openness, which makes the process of citizens' participation in policy making clear; and 3) fairness, which is the consistent and equal treatment of all groups of people. People's trust in institutions is often driven by their perception of corruption. When trust is low, institutions are likely to face more difficulty in establishing integrity; and when society lacks trust and non-cooperative norms, there will be higher tolerance of non-compliance with regulations and laws. In addition, experiences of discrimination also influence perceptions of fairness and trustworthiness of decision makers within the government (Murtin et al., 2018[5]).

A strong belief in government values is important. Several cross-country studies have found that there is a positive link between the level of institutional trust and the quality of the legal system (i.e. the enforcement of property rights protection, accountability or corruption) (Murtin et al., 2018[5]). For example in Switzerland, the higher the democratic participation in cantons, the lower tax evasion. This shows the value of democratic inclusion and engagement in building co-operative behaviour practices.

Table 4.1. Summary of competence-values framework for citizens' trust in public institutions

Trust component	Government mandate	Key elements	Overall public policy objective
Competence: governments' ability to deliver to citizens the services they need, at the quality level they expect	Provide public services	Access to public services, regardless of social/economic condition 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	Use power and 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 for all	Pursuit of socio-economic progress for society at large Consistent treatment of citizens and businesses (vs. fear of capture)	Fairness

Source: OECD (2017[8]), Trust and Public Policy: How Better Governance Can Help Rebuild Public Trust, http://dx.doi.org/10.1787/9789264268920-en.

According to the framework shown in Table 4.1, the five determinants of institutional trust are responsiveness, reliability, integrity, openness and fairness, which can assist governments in restoring, maintaining or increasing the level of public trust. However, for governments to address these issues, they need to focus on delivering public services that meet citizens' needs (see Chapter 3). Consequently, a data-driven approach including citizen engagement, government openness and multi-stakeholder collaboration is necessary.

Indeed, governments are using data to inform policy makers about decision-making processes and to build public value. Many private and public sector organisations rely on data as a resource to not only improve existing products and services, but also to create more innovative ones, gather feedback and most importantly understand users' needs. This implies shifting away from using digital technologies as a simple tool to providing public values driven by them and, particularly data, which also results in the need for good data governance (OECD, 2019[10]).

Good data governance, as discussed in Chapter 2, has the ability to increase the quality of public services. By improving data accessibility and availability, it enables governments to deliver services that are more responsive, reliable, ethical, open and fair. Despite the resulting positive impact on improving citizens' well-being, the extensive use, analysis and collection of data pose pressing, and somehow new, ethical issues. Indeed, the "non-rivalrous" nature of data, which means that it can be copied and used by several people at the same time and for purposes other than those for which the data were collected for, adds more complexity and requires rigorous limitations.

Public trust through data ethics

In the 21st century, data create numerous opportunities to improve policy making, and the design and delivery of public services, and thus contribute to citizens' well-being. Nevertheless, opportunities often come with challenges. The increasing use of, availability and access to data – personal as well as non-personal data – raise a significant number of questions not only about their ethical use, collection, treatment and storage, but also about responsibility, accountability, fairness and the respect of human rights of current legislation in relation to the data.

Citizens' attitudes towards data practices in government are changing fast and their interest in ethical approaches to data management is growing. High-profile data breaches, the influence of tech giants in the private sector and the development of regulations have put the way in which data are handled in the public consciousness. Citizens are increasingly concerned about the way government approaches this area. How data are treated within an organisation depends on how data are viewed and the way data are seen depends, among others, on its leadership (see Chapter 2) and overall culture. Leadership needs to ensure that a culture of responsible data is established. A government's values and culture in using data responsibly are essential for data to be collected, stored and analysed in an ethical and transparent way.

Showing that governments pay attention to each stage of the government data value cycle (see Figure 3.1 in Chapter 3) is key to building trust. Lower trust in government slows policy implementation. Therefore, efforts designed to establish a strong culture of ethical data use are essential to create the enabling conditions that maximise the impact of data-driven practices within public sectors.

Data ethics is a branch of ethics that addresses these challenges in relation to public trust. According to research, data ethics is defined as: *"[…] a new branch of ethics that studies and evaluates moral problems related to data (including generation, recording, curation, processing, dissemination, sharing and use), algorithms (including artificial intelligence, 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 (e.g. right conducts or right values)*" (Floridi and Taddeo, 2016[11]).

The focus on data ethics is becoming increasingly significant, not only because there has been a recent shift from an information-centred approach to a data-centred one (Floridi and Taddeo, 2016[11]), but also because organisations are being called upon to establish their own set of data principles and processes. For the past 30 years, attention was on ethical issues derived from computers and digital technologies. Specific technology such as computers, tablets, cloud computing and so on were the focus of such ethical strategies, whereas today, data ethics is centred on how the technology is used, which refined the approach and contributed to the evolution of computer and information ethics (Floridi and Taddeo, 2016[11]). This emphasises that the resource being handled, data in this case, must be the priority, not the technology using it. The use of data is facilitated when boundaries are set on the use of data in order to draw the best out of it to the benefit of society.

Policy sectors and organisations have been encouraged to develop their own data principles in order to make their practices more ethical and transparent, and thus trustworthy. Indeed, building clear data practices is fundamental to retaining citizens' trust. Correctly handling data can balance innovation with ethical data practices, while placing users at the centre of the product and service design process. For this to happen, citizens need to understand how data about them are being collected, analysed and stored and how long they will be kept for, so that they see the value created from their input, as well as the values and culture of the government handling the data. Consequently, equipping the public to understand and participate in public trust is fundamental as citizens' voice and empowerment is a significant element in nurturing trust and confidence, while adding to digital inclusion (Box 4.1). This brings us back to the idea of the government data value cycle (van Ooijen, Ubaldi and Welby, 2019[12]), which highlights how the different stages data go through can all contribute to maximising its public value (see Chapter 3).

Box 4.1. Christchurch Call to eliminate terrorist and violent extremist content on line

In response to the terrorist attack of 15 March 2019 in Christchurch, New Zealand, New Zealand Prime Minister Jacinda Ardern and French President Emmanuel Macron found a way to engage the public and brought together heads of state and government and leaders from the tech sector to adopt the Christchurch Call.

The Christchurch Call is a commitment by governments and tech companies to eliminate terrorist and violent extremist content on line, while resting on the conviction that a free, open and secure Internet offers extraordinary benefits to society.

Since the attack was livestreamed, went viral and remains available on the web despite the measure taken to remove it, it is important to keep the public informed about the adverse impact of dissemination of such content on line on the human rights of the victims, collective security and people all over the world.

Therefore, significant steps have already been taken by various institutions to address this issue by, among others: the European Commission with initiatives such as the EU Internet Forum; the G20 and the G7, including work underway during France's G7 Presidency on combating the use of the Internet for terrorist and violent extremist purposes; along with the Global Internet Forum to Counter Terrorism; the Global Counterterrorism Forum; Tech Against Terrorism; and the Aqaba Process established by the Hashemite Kingdom of Jordan.

The events of Christchurch highlighted once again the urgent need for action and enhanced co operation among the wide range of actors with influence over this issue, including governments, civil society and online service providers, such as social media companies, to eliminate terrorist and violent extremist content on line.

The call outlines the fact that such an initiative must be consistent with principles of a free, open and secure Internet, without compromising human rights and fundamental freedoms, including freedom of expression. It must also recognise the Internet's ability to act as a force for good, including by promoting innovation and economic development and fostering inclusive societies, which enables governments to maintain their citizens' trust

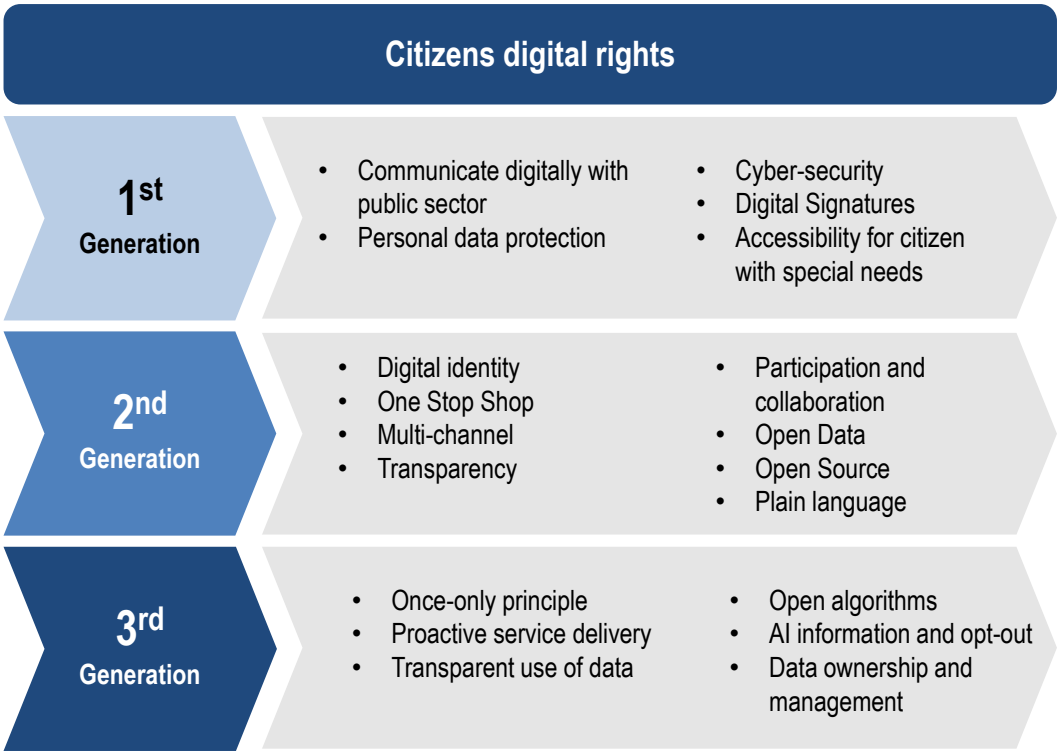
Source: New Zealand Ministry of Foreign Affairs and Trade (2019[13]), Christchurch Call, https://www.christchurchcall.com/call.html.

Digital rights and data rights

Governments are gradually moving towards a citizen-driven transformation enabled by a more sophisticated use of citizens' personal data to offer quality public services. They thus have the responsibility to secure citizens' digital rights. To this end, governments are increasingly strengthening their legal and regulatory efforts to address new issues related to digital rights that are emerging in the digital age. Inspired by the evolution of human rights, Figure 4.2 is a tentative framework that classifies digital rights into first-, second- and third-generation digital rights. These categories are not clear-cut, but simply a way of classification; similarly, most rights may fall under more than one category, which leaves this tentative framework open for discussion.

Similarly to first-generation human rights (civil-political human rights), "first-generation" digital rights should indeed be seen as citizens' fundamental rights, such as personal data protection, the right to communicate digitally with the public sector and cyber security (OECD, 2019[13]) (Figure 4.2).

Figure 4.2. Digital rights – Towards a citizen-driven transformation



Source: OECD (2019[13]), *Digital Government Review of Panama: Enhancing the Digital Transformation of the Public Sector,* https://doi.org/10.1787/615a4180-en.

For example, the Mexican Constitution enacted Internet access as part of the human rights and guaranteed strict impartiality in 2013 (Freedom House, 2018[14]). Another example is the Digital Single Market strategy proposed by the European Commission in 2015, where 17 legislative proposals have been accepted and 12 more are awaiting (European Commission, 2019[15]). European citizens have been enjoying the right to access Internet freely without being discriminated for their choice of content since 2016, and to access their TV, sports and music subscriptions free of charge when traveling within the EU since 2018.

However, due to the fast development of technology, including the rapid spread across governments of emerging technologies such as artificial intelligence, it becomes essential for governments to address "second-generation" (socio-economic human rights), and even "third-generation" (collective developmental human rights) digital rights (OECD, 2019[13]), revisiting the existing understanding of digital rights and related legal measures. On average, most OECD countries have a government that covers "second-generation" digital rights. In Panama, for example, the government took less than a decade to adopt a digital rights-oriented approach. Many laws, such as the right of citizens to digitally interact with public sector organisations (Asamblea Nacional, 2012[16]), the application of the once-only principle, the national policy on open government data (Asamblea Nacional, 2012[16]) (Ministerio de la Presidencia, 2017[17]) and personal data regulation (Asamblea Nacional, 2019[18]) were passed. More country examples are given later in this chapter.

Across the European Union, there are implications from the introduction of the EU's General Data Protection Regulation (GDPR) in 2018. Created with the goal of protecting EU citizens from data and privacy breaches, it has resulted in changes to existing law as well as new introductions. In Portugal, this has resulted in a high-level priority initiative to consider any additional regulations or adaptions required to address those issues, which are devolved to member states.

Recognising and finding ways to protect digital rights is necessary, but insufficient to create a safe environment and build mutual trust. Legal and regulatory measures must be paired with soft principles, e.g. guidelines, to be adopted by governments and be used broadly across public sectors. To respond to this, specific actions on data-related rights and legal pieces, which will be discussed in the next section, have been taken by countries. In addition, the OECD is developing some data ethical guidelines in collaboration with its member countries, also discussed further in this chapter. In order to build trust, regulatory practices and principles address the four areas of ethics, privacy and consent, transparency, and security.

Good data-related legislation across OECD countries

Many governments seem to have placed ethics, privacy and consent, transparency, and security as high priorities and have taken a legalistic approach to address them. Although the role of governments is to protect citizens' data and ensure fundamental rights and freedom of citizens whose data are being used are respected, governments also prioritise based on the needs of their citizens and the challenges they face. For this, many regulatory efforts have been undertaken to make the process transparent and accessible.

In **Korea** for example, the Personal Information Protection Commission is required by law to establish a master plan every three years to ensure the protection of personal information and the rights and interests of data subjects. Furthermore, the heads of central administrative agencies must establish and execute an implementation plan to protect personal information each year in accordance with the master plan. On an ongoing basis, any change to policy, systems or statutes requires an assessment of the possibilities of data breaches, which are then openly published (Government of Korea, 2019[19]). This approach shows that privacy and transparency were pressing issues to address in Korea.

The **United Kingdom**, which has moved quickly to respond to technological developments, ensures that legislation (for example, the Digital Economy Act and the Data Protection Act) is in step with innovation to ensure personal data and citizen privacy is protected. This demonstrates that the United Kingdom's digital agenda consistently tempers the potential of new forms of technology with caution around the use of personal data. This involves both external experts from civil society, and convenes a number of departmental groups, to ensure that data work is adequately scrutinised and that data protection and privacy regimes are robustly upheld.

Portugal chose to prioritise security as one of the guiding principles of its ICT Strategy 2020 as "data security, resilience and privacy". Portugal has implemented initiatives to reduce the risks associated with digital security. The National Commission for Data Protection has the responsibility to ensure that data protection laws are being applied, and as a result digital security is being acknowledged. This complements the work of the National Security Cabinet of Portugal, which guarantees the security of classified information and is responsible for authorising individuals and companies to access and manipulate this information. Additionally, the National Cybersecurity Centre ensures Portugal uses the Internet in a free, reliable and secure way.

Although governments use different approaches to address trust challenges in their country, there is a consistency to their efforts in addressing four areas while considering their operations and activities. These four areas emerged in research, digital government reviews and reports (Welby, 2019[20]; van Ooijen, Ubaldi and Welby, 2019[12]; OECD, forthcoming[21]), which argue that trust is built and maintained through the following areas:

- ethics: ethical approaches to guide behaviours across the public sector
- privacy: protecting the privacy of citizens and establishing rights to data
- transparency: transparency and accountability of algorithms used for public decision making
- security: managing risks to government data.

Ethics

Ethics refers to ways data are handled without harming anyone directly or indirectly, even if the distribution of data is lawful. This is not only a broad aspect, as this concept addresses an umbrella of all dimensions of the framework, but it is also vital to note that unethical is not necessarily unlawful. For example, publishing personal data on abortion providers' information such as name, clinic and date in a place where it is considered as non-acceptable and where women are likely to be victims of violence would be unethical, although the publication of information is allowed (ODI, 2017[22]). This shows that it is essential for governments to adopt an ethical initiative, aimed at guiding decision making and informing behaviour around data.

Several countries have formal requirements articulating their principles for gathering, processing, sharing, accessing and reusing data in order to prevent, and sanction, any behaviour outside of the public interest. Legislation is one route to ensuring ethical management and use of personal information in both the public and private sectors. In support of this, the Personal Information Protection Portal (Korean Ministry of the Interior and Safety, 2019[23]) was established in Korea to raise public awareness of the issue and is providing online education opportunities offering customised programmes for individuals and businesses to raise their awareness on ethical management and the use of data. This is supported by the development of ten principles for citizens, and businesses, to prevent any personal information violations. In the case of businesses, evaluations are carried out to identify whether they are following the requirements and principles of personal information protection, de-identification of personal information, providing technical assistance, and managing identification information (Korean Ministry of Public Administration and Security, 2019[24]).

However, it is important to note the increasing focus on establishing ethical frameworks as a way to avoid setting regulations. Since ethics is often considered as an "easy" or "soft" option to self-regulate digital practices, many private organisations use it for decision-making procedures, for example:

> *As part of a panel on ethics at the Conference on World Affairs 2018, one member of the Google DeepMind ethics team emphasised repeatedly how ethically Google DeepMind was acting, while simultaneous avoiding any responsibility for the data protection scandal at Google DeepMind (Powles and Hal, 2018[25]). In her understanding, Google DeepMind was an ethical company developing ethical products and the fact that the health data of 1.6 million people was shared without a legal basis was instead the fault of the British government. (Wagner, 2018[26])*

Dr. Wagner argues that it is fundamental to have criteria against which the application of ethics can be measured. In case these common criteria are not respected, there is a risk that many ethical frameworks become "arbitrary, optional or meaningless rather than substantive, effective and rigorous" (Wagner, 2018[26]).

In order to enforce ethical practices, countries have established independent bodies and developed frameworks around the management and use of data. The following country practices illustrate the various ways of creating an ethical environment.

Ethics through an independent entity

Governments can promote ethical behaviour through a lead agency for government-held data. Its role is to support government entities to build their capability and manage the data they hold about citizens as a valuable strategic asset, to ease access of data, to implement data standards and experiment with new methodologies. To illustrate this, **Ireland** and **Portugal** have established particular organisations to take ownership of this agenda.

In **Ireland**, it is the Office of the Data Protection Commissioner (Data Protection Commission, 2019[27]) and in **Portugal** the National Commission for Data Protection (CNPD) is an independent entity with powers of authority extending throughout the country. It supervises and monitors compliance with the laws and

regulations in the area of personal data protection, with strict respect for human rights and the fundamental freedoms and guarantees enshrined in the Constitution and the law. For instance, public and private entities have to notify the CNPD regarding any personal data treatment they make.

This route to implement ethical behaviour is especially common in countries with indigenous populations. Since data about indigenous people is a "complex legal and ethical terrain" (Australian National Data Service, 2019[28]) which needs to be managed with care, a lead agency for government-held data ensures that the data are indeed handled ethically. The Alberta First Nations Information Governance Centre is an example. A regional satellite of the National Centre in **Canada** was established by First Nations to meet Alberta First Nations Information Governance Centre needs. It is the first indigenous model of research and aims at facilitating the exercise of First Nations jurisdiction and giving ownership, control, access and possession of First Nations data and information. The model prioritises culturally relevant indicators as they realised that some indicators may be either irrelevant for communities while interpreting data or unable to inform effective government policy (Healy, 2012[29]).

Having an independent entity also enables ideas to be tested, strategies to be set and risks to be measured. **New Zealand**'s State Services Commissioner designated the chief executive of Stats NZ as the government chief data steward in 2017. As the lead for data, the government chief data steward's role is to set the strategic direction for the government's data management. This is done by supporting government agencies to build their capability and realise the value of the data they hold as a strategic asset (Box 4.2).

Box 4.2. New Zealand: Data Ethics Advisory Group

In order to balance increased access and use of data with appropriate levels of risk mitigation and precaution, the government chief data steward in New Zealand founded the so-called Data Ethics Advisory Group, whose main purpose is to assist the New Zealand government in understanding, advising and commenting on topics related to new and emerging uses of data.

To ensure the advisory group delivers on its purpose, the government chief data steward has appointed seven independent experts from different areas relevant to data use and ethics as members, including experts in privacy and human rights law, technology, and innovation. One of the member positions is reserved for a member of the Te Ao Maoru Co-Design Group as means to support the Maori data governance work and include different perspectives in the New Zealand data governance framework.

The group is solely to discuss and comment on subjects and initiatives related to data use, not broader digital solutions by public bodies. Examples of topics that the Data Ethics Advisory Group might be requested to comment on include the appropriate use of data algorithms (e.g. how to avoid algorithmic bias) and the correct implementation of data governance initiatives.

Source: Stats NZ (2019[31]), Data Ethics Advisory Group, https://www.data.govt.nz/about/government-chief-data-steward-gcds/data-ethics-advisory-group (accessed on 27 August 2019).

Ethics through an ethical framework or guidelines

Another way governments can establish ethical behaviours is through a framework or guidelines, which provides users with information, resources and approaches to help them achieve ethical practices and decision making. The framework and guidelines are not intended to be prescriptive, but aim at widening a common understanding and to work through ethical concerns.

In the **United Kingdom**, the codes of practice for the use of data-sharing provisions within the Digital Economy Act contain checks and balances consistent with the Data Protection Act, to ensure data are not

misused or shared indiscriminately (Department for Digital, Culture, Media & Sport, 2019[30]). For data work outside the scope of legislation, the Data Ethics Framework has been developed and continues to be iterated upon, to guide policy makers and data analysts in the ethical implications of the work they are undertaking (Box 4.3).

Another example is **New Zealand**. The Government Chief Data Steward and the Privacy Commissioner have jointly developed six key principles to support safe and effective data analytics, including the Privacy, Human Rights and Ethics (PHRaE) Framework. Established by the Ministry of Social Development, the PHRaE Framework is a set of capability and tools with which users of information interact to ensure that people's Privacy (P), Human Rights (HR) and Ethics (E) are considered from the design stage of a new initiative (Box 4.3).

Box 4.3. United Kingdom: Data Ethics Framework

In 2018, the United Kingdom established a Data Ethics Framework to guide public servants in the appropriate use of data. Public servants should assess each project, service or procured software against the seven data ethics principles below, which are designed to be regularly reiterated:

1. Start with clear user need and public benefit. Using data in more innovative ways has the potential to transform how public services are delivered. We must always be clear about what we are trying to achieve for users – both citizens and public servants.
2. Be aware of relevant legislation and codes of practice. You must have an understanding of the relevant laws and codes of practice that relate to the use of data. When in doubt, you must consult relevant experts.
3. Use data that are proportionate to the user need. The use of data must be proportionate to the user need. You must use the minimum data necessary to achieve the desired outcome.
4. Understand the limitations of the data. Data used to inform policy and service design in government must be well understood. It is essential to consider the limitations of data when assessing if it is appropriate to use it for a user need.
5. Ensure robust practices and work within your skill set. Insights from new technology are only as good as the data and practices used to create them. You must work within your skill set, recognising where you do not have the skills or experience to use a particular approach or tool to a high standard.
6. Make your work transparent and be accountable. You should be transparent about the tools, data and algorithms you used to conduct your work, working in the open where possible. This allows other researchers to scrutinise your findings and citizens to understand the new types of work we are doing.
7. Embed data use responsibly. It is essential that there is a plan to make sure insights from data are used responsibly. This means that both development and implementation teams understand how findings and data models should be used and monitored with a robust evaluation plan.

Source: Department for Digital, Culture, Media & Sport (2018[33]), Guidance Data Ethics Framework, https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework#the-data-ethics-framework-principles.

Additionally to ensuring public servants' ethical behaviour when handling citizens' data, the increasing usage of emerging technologies by governments to improve public services and government programmes also introduces another set of ethical behaviours. Due to the complexity of artificial intelligence (AI) systems, it is crucial to ensure the effective and ethical use of AI. The federal government of **Canada** explored the responsible use of AI in government, established an Algorithmic Impact Assessment (AIA) tool in order to assist designers evaluate the suitability of their AI solutions and created a set of guidelines

to complement it (Box 4.4). The AIA is a questionnaire designed to help companies and governments assess and mitigate the risks associated with deploying an automated decision system. The AIA also helps identify the impact level of the automated decision system under the Directive on Automated Decision-Making. The questions are focused on business processes, data and system design decisions (Government of Canada, 2019[31]).

Box 4.4. Canada: Guiding principles complementing the Algorithmic Impact Assessment

Although emerging technology is very often used to help governments take better informed decisions, governments need to ensure that they are appropriately used with citizens' best interests in mind. Therefore, the government of Canada put in place a set of artificial intelligence (AI) guiding principles to guarantee the effective and ethical use of AI, complementing the Algorithmic Impact Assessment (AIA) tool.

In the Canadian government, all public servants need to follow the guidelines below before applying AI:

1. Understand and measure the impact of using AI by developing and sharing tools and approaches.
2. Be transparent about how and when they are using AI, starting with a clear user need and public benefit.
3. Provide meaningful explanations about AI decision making, while also offering opportunities to review results and challenge these decisions.
4. Be as open as they can by sharing source code, training data and other relevant information, all the while protecting personal information, system integration, and national security and defence.
5. Provide sufficient training so that government employees developing and using AI solutions have the responsible design, function and implementation skills needed to make AI-based public services better.

Source: Government of Canada (2019[36]), Responsible Use of Artificial Intelligence (AI), https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/responsible-use-ai.html.

These country examples have demonstrated that establishing an ethical environment is fundamental to developing further ethical initiatives and that there are different ways to do so. Since these approaches are not exclusive in their contribution to public trust, it is common to see some countries like Canada and New Zealand using more than one to enforce their ethical practices and behaviours.

Privacy and consent

Privacy is a concept that applies to data subjects while confidentiality applies to data. Regarding consent, this is the concept of "informed consent", where the individual whose data are being collected is aware of the purpose of the data collection and agrees to give data about them for these purposes (OECD, 2016[32]). This area is surely a priority as citizens are very likely to approach the breach of privacy and consent negatively, especially in terms of sensitive data. They may not be aware of the value of making data about them accessible as discussed in Chapter 3 and may fear that they are being "watched" by the state.

Therefore, failure to consider privacy and/or consent can create tensions and challenges. For example, Moorfields Eye Hospital and DeepMind, who partnered to explore AI solutions to improve patients eye care, were found to have committed major breaches of contract, such as processing and storing data at locations not mentioned in the data-sharing agreement; sharing data with third parties without clear

consent; as well as several failures of security and operational procedure (PrivSec Report, 2019[33]). Such incidents can have an adverse impact on their reputation and they can thus lose trust from current and potential patients.

Consequently, countries have set formal requirements, including legislation, to protect citizens across data collection, storage, sharing and processing and, data opening, release and publication. In order to address issues relevant to privacy and consent, some governments have established data rights for businesses and citizens. Namely, they provide access to:

- which data government organisations hold about them
- which public organisations have the right to access their data
- which public organisations have made use of their data and for what purposes
- which public organisations have made an enquiry about their data
- the right to provide (personal) data only once to the government
- the right to agree or refuse permission for data they provide to one public institution to be shared with and reused by others.

In the case of **Canada** and the **United Kingdom**, they have consistently done so for both citizens and businesses. They have established practical mechanisms by which citizens and businesses can exercise the right to know which data government organisations hold about them. This is handled through Freedom of Information legislation in the United Kingdom and under the Privacy Act and Access to Information Act in Canada.

Similarly, in **Korea**, they also have rights to data for both citizens and businesses, with the exception of the right to know which public organisations have the right to access their data, which is established only for citizens. Businesses are therefore unable to establish which public organisations have the right to access their data. The Personal Information Protection Act (National Law Information Center, 2019[34]) details principles for collecting, processing and sharing of personal information. The second piece of legislation, the Act on Promotion of the Provision and Use of Public Data (Open Data Act) (National Law Information Center, 2019[35]) establishes the principles for an ethical approach to data sharing, access and reuse. Between them, these laws seek to ensure universal access to data use, equality in data access and prohibition of activities impeding the use of public data.

In May 2018, the General Data Protection Regulation (GDPR) applied in all EU countries with the aim of protecting European citizens from privacy and data breaches. Although very similar to the previous data protection acts, this regulation has strengthened conditions for consent, which means that companies can no longer use data that the data subject has not agreed on. It also stated that consent has to be given in a clear and easily accessible form, with the option to withdraw. Besides this, the regulation also has given extensive rights to data subjects, such as the right to access, edit, be forgotten, restrict processing and data portability (Box 4.5) (EU GDPR.ORG, 2019[36]). Since the GDPR applies all across the EU, European countries are collectively addressing this issue of privacy through the transposition of EU directives into their national laws.

In **Portugal**, it is possible for citizens and businesses to query data and in some specific cases, to consent and refuse permission for the citizen or business data they provide to a given public sector organisation to be shared with and reused by other public sector organisations.

In **Spain**, citizens have had the right to know which data government organisations hold about them since 2015. Citizens have the right to know all of the information, at any time, as well as the status of the processing of the procedures which concern the citizen. Additionally, citizens have the right to access and copy the documents contained in the aforementioned procedures. The GDPR reinforces the need for consent for data processing. The availability of such data is strictly limited to those that are required from the citizens by the other administrations for the actions within their field of competence, in accordance with the regulations thereof.

Box 4.5. General Data Protection Regulation: Data subject rights

Right to access - Part of the expanded rights of data subjects outlined by the European Union's General Data Protection Regulation (GDPR) is the right for data subjects to obtain confirmation from the data controller as to whether or not personal data concerning them are being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

Right to rectification - Individuals have the right to have inaccurate personal data rectified. An individual can also have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

Right to be forgotten - Also known as data erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure include the data no longer being relevant to the original purposes for processing, or a data subject withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Right to restrict processing - Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting to do so. This may be because they have issues with the content of the information being held or how their data have been processed. In most cases, an individual will not be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time.

Data portability - The GDPR introduces data portability – the right for a data subject to receive the personal data concerning them – which they have previously provided in a "commonly used and machine-readable format" and have the right to transmit those data to another controller.

Source: EU GDPR.ORG (2019[41]), GDPR Key Changes, https ://eugdpr.org/the-regulation.

Before the application of the GDPR, the right to access was somehow limited in some European countries. For example, **Denmark** and **Sweden** enacted limited rights. Denmark established one right, for citizens and businesses to access the data which government organisations hold about them. This right for those actors also existed in Sweden, with citizens also having the right to know which public organisations have the right to access their data. Denmark enabled citizens in certain cases to know which data government organisations hold about them through the websites www.borger.dk and www.sundhed.dk. Additionally, the Basic Data Programme established the principle that citizens and businesses should only have to provide personal data once to government, obliging them to share and reuse these data.

Since all EU countries are compliant with the legislation, this has also influenced countries outside of the EU. For instance, immediately after the GDPR went into effect, **Japan** followed with an agreement with the European Union on a reciprocal recognition of an adequate level of protection for personal data. Japan is the first country receiving such an adequacy decision from the European Commission, which not only guarantees a smooth flow of data between Japan and the EU, but also makes heavy data transfers, trade and partnerships easier (PrivSec Report, 2019[37]).

Although the coverage of data rights varies from country to country, the application of the GDPR put individual and business data rights under a greater spotlight. Before the legislation, the right to data access was more or less covered by countries. Whereas, the GDPR introduces on top of the right to access, the right to edit, remove and restrict, which highly contributes to public trust.

Transparency

Transparency is an environment in which the objectives of policy; its legal, institutional and economic framework; policy decisions and their rationale; data and information related to monetary and financial policies; and the terms of agencies' accountability, are provided to the public in a comprehensible, accessible and timely manner (OECD, 2019[38]).

Since governments start integrating emerging technologies in their decision process, data used to feed into AI systems are essential. However, citizens often are not informed about the data being used, how and by whom (Saidot, 2019[39]). This is why transparency of data ensures the high-quality and reliability of data (OECD, forthcoming[40]), which is fundamental to the successful implementation of machine learning, other applications of artificial intelligence and to maintain trust.

As countries consider the role that AI can play in replacing the decision-making activities of public servants, it is necessary to understand how governments might audit their decision-making processes and analyse the outcomes, which affect citizens' lives. Consequently, it is important that countries take steps to make their decision-making algorithms transparent.

Exposing the behind-the-scenes of an algorithm is a powerful way to strengthen trust from users, to correct errors and avoid biases. The transparency of algorithms can not only help the AI community improve, but also enforce individual data rights, which according to the GDPR means that individuals have the right to be informed about the collection and use of data about them as well as "the details of the existence of automated decision making, including profiling" (Information Commissioner's Office, 2019[41]).

The French Lemaire Act was voted to serve this purpose for greater transparency in 2016. It aims at ensuring a trustworthy public service of data in France by encouraging innovation and building a framework of trust that guarantees the rights of users while protecting their personal data (Dreyfus, 2019[42]).

In the **United Kingdom**, for example, the Data Ethics Framework provides a foundation to the work being done in the field of data science, with Principle 6 identifying that all activity should be as open and accountable as possible (Department for Digital, Culture, Media & Sport, 2019[30]). While the framework is not mandated in any formal way, it is in keeping with the way in which the United Kingdom has disseminated best practices throughout the public sector in terms of the Service Standard and the Service Manual. Supporting this framework is the commissioning of the UK Office for Artificial Intelligence to explore the use of algorithms and other techniques such as machine learning in government transformation and to aid decision making. The UK government also collaborates with external academic and research institutions in industry, including the Alan Turing Institute, the Open Data Institute, the Open Government Partnership and Policy Lab.

New Zealand has recently developed the Principles for Safe and Effective Use of Data and Analytics, which aim at providing good practices, and supporting agencies that use algorithms in decision making. This also ensures that New Zealanders are informed and have confidence in how the government uses algorithms (New Zealand Government, 2019[43]).

In **Korea**, the "Public Sector Big Data Analysis Project" has been supporting data-driven, scientific administration of the central government, local governments and public institutions since 2014.

Although governments establish frameworks or principles to set standardised information and make communication and use of data clearer to enhance transparency, the way in which governments open themselves to scrutiny both on their published performance and also as an ongoing culture and in terms of their democratic norms and principles is also a way of gaining trust.

Indeed, some countries use transparency as a practical device and pair their digital approaches with practical mechanisms for citizens to understand how their data are being used, which helps citizens see governments acting to build trust (OECD, 2019[44]). Giving control of data and/or showing ways in which

data are used to citizens are important aspects to ensure citizens' confidence in services, and thus government.

In the case of digital identity, Spain with *Carpeta Ciudadana* and Denmark with *NemID* offer citizens the ability to control data about them as well as the ability to see the details of how their data are being accessed and used on line (OECD, 2019[44]). Increasingly countries are empowering citizens with a website that enables them to see their own login activity and information about the way organisations have been using their data, and also to grant and revoke permission for use of the data.

Security

Security refers to the measures taken to prevent unauthorised access or use of data (OECD, 2019[38]). The importance of data management in governments is not only relevant in relation to how it can be applied and made use of to design better policies and to improve services, but also in how it preserves the privacy of citizens and their trust. Citizens need to know that efforts are being made to ensure that their privacy is respected and that they can trust government to handle their personal information, and to protect them from potential risks associated with how governments handle those data.

Failure to patch computers across the world can have devastating effects for both the private and public sectors. Digital security attacks can be extremely costly not only in terms of financial cost, but also in terms of reputation. Indeed, an organisation suffering from a data breach can lose its users' trust, as well as that of potential users (IT Governance, 2019[45]).

Indeed, the prospect of digital security attacks which cripple infrastructure and damage the ability for citizens to access services is not a hypothetical risk, but a reality. In May 2017 the WannaCry ransomware attack affected companies and individuals in over 150 countries, including FedEx, Renault-Nissan and the United Kingdom's National Health System. The following month NotPetya caused an estimated USD 10 billion of damage. Both attacks exploited a penetration tool known as EternalBlue created, and leaked, by the United States National Security Agency. While a patch to safeguard against EternalBlue would have mitigated the impact of WannaCry, the evolution of NotPetya meant it was capable of infecting computers which had been patched. Nevertheless, this highlights the importance for governments, businesses and citizens to take their information security seriously (Welby, 2019[20]).

Therefore, digital security is not an optional extra, but must be a fundamental part of government strategies around digital, data and technology. It also needs to be approached in ways that enable the proactive use of data for designing and delivering better quality government. As enforced in the GDPR, organisations need to make digital security a priority by implementing appropriate technical and organisational measures to protect the data they hold. Failure to do so can lead to heavy fines (IT Governance, 2019[45]).

Many countries identify digital security as a high priority on their country's digital government agenda. This is why many have developed strategies and policies for the management of security risks related to government data and information. Countries such as **Korea** and the **United Kingdom** have standalone digital security strategies while Ireland recognises it as part of an additional strategy.

Korea identified a standalone policy that focuses on best practices around using and regulating data in order to offset the threats of digital security. The National Information Resources Service manages all government servers and databases in accordance with this security policy, bringing the issue under central oversight.

The **United Kingdom** not only has a specific chapter on digital security within its national Digital Strategy, but a specific National Cyber Security Strategy 2016-2021 as well. Both documents discuss the ambition of making the United Kingdom the safest place in the world to live and work on line. The National Cyber Security Centre aims to build effective cyber security partnerships between government, industry and the public to ensure that the United Kingdom is safer on line. It provides cyber incident response, liaison with

the United Kingdom's security services and acts as the United Kingdom's authoritative voice on cyber security. For the first time, those working in government and the private sector have been given a route for directly engaging with the country's cyber security professionals in order to access the best possible advice and support on securing networks and systems from digital security threats.

Although **Ireland** does not have a standalone strategy, it is making digital security a priority for the broader policy agenda with digital security being one of the five pillars of its Public Service ICT Strategy.

Nevertheless, digital security is an area that is already being addressed either in countries' standalone strategy or their broader policy agenda, but providing the public with digital security skills is equally as important. Investing in citizens' digital security skills is also necessary. Not only for government to protect itself, but also in 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.

Organisations around the world identified a digital security skill gap in various industries. A McAfee report stated 82% of responding countries (Australia, France, Germany, Israel, Japan, Mexico, the United Kingdom and the United States) noted a shortage of digital security skills in their country (Center for Strategic and International Studies, 2016[46]). Furthermore, the UK government commissioned a study to define the basic technical digital security skills gap and found that 54% of private sector and non-profit organisations and 18% of public sector organisations have such a gap (Department for Digital, Culture, Media & Sport, 2019[47]; Pedley et al., 2018[48]). Given the rapid advancement of technology, digital economy and digital threats, such a large skill gap becomes a pressing issue. Despite the complexity of understanding the nature and evolution of digital security skills over time, countries like the United Kingdom have started addressing this matter along with its National Cyber Security Strategy, further discussed in Box 4.6 (Department for Digital, Culture, Media & Sport, 2019[47]).

Box 4.6. Increasing the United Kingdom's cyber security capability

The United Kingdom initially established a National Cyber Security Strategy to ensure that "the UK has a sustainable supply of home-grown cyber skilled professionals to meet the growing demands of an increasingly digital economy, in both the public and private sectors, and defence". However, due to the increasing demand of digital security skills, it now seeks to go much further.

The government's ambition is to address the broader cyber security capability gap: ensuring the right skilled professionals are in the workforce now and in the future; that organisations and their staff are equipped to manage their cyber risks effectively; and that individuals have an understanding of the value of their personal data and are able to adopt basic cyber hygiene to keep themselves and the organisations they work for protected.

Its mission is therefore to increase cyber security capacity across all sectors to ensure that the United Kingdom has the right level and blend of skills required to maintain resilience to cyber threats and be the world's leading digital economy.

It will pursue its mission by working toward the following objectives:

- to ensure the United Kingdom has a well-structured and easy to navigate profession which represents, supports and drives excellence in the different cyber security specialisms, and is sustainable and responsive to change
- to ensure the United Kingdom has education and training systems that provide the right building blocks to help identify, train, and place new and untapped cyber security talent

- to ensure the United Kingdom's general workforce has the right blend and level of skills needed for a truly secure digital economy, with UK-based organisations across all sectors equipped to take informed decisions about their cyber security risk management
- to ensure the United Kingdom remains a global leader in cyber security with access to the best talent, with a public sector that leads by example in developing cyber security capability.

Source: Department for Digital, Culture, Media & Sport (2019[52]), Initial National Cyber Security Skills Strategy: Increasing the UK's Cyber Security Capability - A Call for Views, Executive Summary, https://www.gov.uk/government/publications/cyber-security-skills-strategy/initial-national-cyber-security-skills-strategy-increasing-the-uks-cyber-security-capability-a-call-for-views-executive-summary#fn:1

Data ethics guidelines

Recognising the commonality of the issues and challenges being addressed, governments worldwide have started looking into sharing best practices in the development of ethical frameworks so as to develop a common set of principles. This would contribute to fostering a stronger culture for ethical use of data across countries. This is extremely relevant as in an increasingly digital world, data flows and sharing between countries are seen as a way to improve service delivery to globalised citizens, and to strengthen international collaboration to fight common policy issues. The OECD Thematic Group on DDPS is a key example of this joint endeavour (Box 4.7).

Aimed at policy makers, statisticians, analysts, data scientists and any public officers handling data, these guidelines seek to encourage public servants to work together and design appropriate use of data. The proposed ethical guidelines discussed in Box 4.7 act as a response to ethical behaviours, digital rights and data rights' challenges. Although laws and regulations around the rights of citizens, the behaviour of public servants, and the application of data and technology already inform the activity of government, it is necessary to pair them with ethical guidelines to ensure ethical practices, consistency of conduct and maintain trust.

Box 4.7. Proposed ethical guidelines

Led by the Netherlands, the OECD Thematic Group on Data-Driven Public Sector (DDPS) agreed on the following ethical guidelines in June 2019 during the 5th Expert Group Meeting:

Data in a DDPS and the use thereof should serve public value. The collection and use of data by governments must strengthen the institutions of democracy and the rule of law.

Governments using data in an ethical way to improve public services quality and increase public value, while strengthening democratic standards and avoiding discrimination, must be the norm.

Be clear about the purpose of specific data use. Make sure that data use has a clear articulated purpose that explains the reason why data are being used and that addresses the concerns of different stakeholders.

All parties of the data value cycle should plainly understand the goal, which should be articulated ex ante, of every use of data and at every stage. From the way it is designed, the purpose it serves, the need it is meeting and the benefits it is searching for must be clear to all stakeholders involved, so that the right to be informed is applied, quality and trust can be guaranteed all along the process and every use of data explained.

Define boundaries for use. Make sure that the design considers balanced data use by weighing relevant societal costs and benefits with data minimisation as the norm when it comes to personal data. This ensures the quality of design and the ability to explain how data are being used.

Governments should define boundaries of the use of data, which promotes transparency. They should collect and use the sufficient amount of non-biased data that would enable them to complete their tasks. Any abuse of data usage could lead to negative consequences, such as losing citizens' trust in public servants.

Use data with integrity. Government should not abuse its position, the data at its disposal or the trust of the public.

Governments should use data in a responsible way in order to enhance trust. Due to the opportunities and values that data can bring, the government's strategic shift to a data-centric approach puts the design and delivery process of public services under the spotlight. Since data used by governments to improve the quality of services is highly sensitive, this not only requires a careful consideration, but also a secure treatment and an ethical behaviour from public servants handling those data.

Be accountable. Governments design mechanisms for giving citizens insight into and consent for the use of their personal data by organising internal and external accountability. Stakeholders should know where to address questions, remarks or mistakes and governments should be responsive to the input of citizens.

Accountability is not just about disclosing how personal data are being handled and publishing public data, but also about being transparent with government activities and having strong enough digital security to protect government-held data. This enables citizens to have stronger confidence and witness their contribution to public services.

Be understandable and transparent. Government is transparent in terms of how data are being collected and used, and communicates clearly and in understandable ways about the role of data, including algorithms, in the provision of public goods and services. Government data are open data unless they conflict with legitimate privacy, economic or security concerns.

For every use of data, governments should be transparent and should communicate efficiently the purpose of such use and how data are being treated. The right to be informed must be a fundamental data right because it helps governments deal with people in a clear and transparent way and empower them, which is key to developing citizens' trust in government.

Broaden citizens' control over personal data. Citizens are empowered and have action perspective because of gained knowledge to take decisions about the sharing of their personal data within, or external to, government.

Empowering citizens by giving them more control over their personal data proves that governments put citizens at the centre and value their participation. This should give them the right to be informed, access, modify, delete and restrict data, data portability, to object and rights related to automated decision making.

Avoid discrimination and support inclusion. The applied use of data should recognise, and mitigate, any potential bias so that it never leads to discrimination, with people in similar cases always treated equally.

In order to treat data in a responsible way and avoid biased data, public servants need to be equipped with the appropriate technical skills to be able to identify errors and biased situations.

References

Aberbach, J. (2007), "Citizens and consumers", *Public Management Review*, Vol. 7/2, pp. 225-246, http://dx.doi.org/10.1080/14719030500091319. [9]

Ahn, S. and P. Hemmings (2000), "Policy Influences on Economic Growth in OECD Countries: An Evaluation of the Evidence", *OECD Economics Department Working Papers*, No. 246, OECD Publishing, Paris, https://dx.doi.org/10.1787/581718238837. [4]

Asamblea Nacional (2019), *Ley 81 de 26 de marzo de 2019 - De protección de datos personales*, https://www.gacetaoficial.gob.pa/pdfTemp/28743_A/GacetaNo_28743a_20190329.pdf. [18]

Asamblea Nacional (2012), *Ley 83 de 9 de Noviembre de 2012 - Regula el uso de medios electrónicos para los tramites gubernamentales*, http://www.innovacion.gob.pa/descargas/Ley_83_del_9_de_noviembre_2012.pdf. [16]

Australian National Data Service (2019), *Indigenous Data*, https://www.ands.org.au/working-with-data/sensitive-data/indigenous-data. [28]

Center for Strategic and International Studies (2016), *Hacking the Skills Shortage: A Study of the International Shortage in Cybersecurity Skills*, McAfee, https://www.mcafee.com/content/dam/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf. [46]

Data Protection Commission (2019), *The Data Protection Commission*, https://www.dataprotection.ie. [27]

Department for Digital, Culture, Media & Sport (2019), *Guidance Data Ethics Framework*, Department for Digital, Culture, Media & Sport, London, https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework. [30]

Department for Digital, Culture, Media & Sport (2019), *Initial National Cyber Security Skills Strategy: Increasing the UK's Cyber Security Capability - A Call for Views, Executive Summary*, Department for Digital, Culture, Media & Sport, London, https://www.gov.uk/government/publications/cyber-security-skills-strategy/initial-national-cyber-security-skills-strategy-increasing-the-uks-cyber-security-capability-a-call-for-views-executive-summary#fn:1. [47]

Department for Digital, Culture, Media & Sport (2018), *Guidance Data Ethics Framework*, Department for Digital, Culture, Media & Sport, London, https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework#the-data-ethics-framework-principles. [53]

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. [42]

EU GDPR.ORG (2019), *GDPR Key Changes*, https://eugdpr.org/the-regulation. [36]

European Commission (2019), *Digital Single Market*, European Commission, https://ec.europa.eu/digital-single-market/en. [15]

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. [11]

Freedom House (2018), *Mexico*, https://freedomhouse.org/report/freedom-net/2018/mexico. [14]

Government of Canada (2019), *Algorithmic Impact Assessment (AIA)*, https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/responsible-use-ai/algorithmic-impact-assessment.html. [31]

Government of Canada (2019), *Responsible Use of Artificial Intelligence (AI)*, https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/responsible-use-ai.html. [52]

Government of Korea (2019), *Personal Information Protection Commission*, http://www.pipc.go.kr/cmt/main/english.do. [19]

Healy, B. (2012), *The Alberta First Nations Information Governance Centre*, Alberta First Nations Information Governance Centre, Alberta, https://www.fnhma.ca/archive/conference/2012/files/Bonnie_Healy.pdf. [29]

Information Commissioner's Office (2019), *Right To Be Informed*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/. [41]

IT Governance (2019), *What is Cybersecurity?*, https://www.itgovernance.co.uk/what-is-cybersecurity. [45]

Korean Ministry of Public Administration and Security (2019), *10 Commandments to Prevent Misuse of Personal Information*, https://www.privacy.go.kr/nns/ntc/cmd/tenCommandments.do. [24]

Korean Ministry of the Interior and Safety (2019), *Personal Data Protection Laws in Korea*, https://www.privacy.go.kr/eng. [23]

McKnight, D. and N. Chervany (2000), "What is trust? A conceptual analysis and an interdisciplinary model", *AMCIS 2000 Proceedings*, Vol. 382, http://aisel.aisnet.org/amcis2000/382. [1]

Ministerio de la Presidencia (2017), *Decreto ejecutivo 511 de 24 de noviembre de 2017 - Adopta la politica pública de transparência de datos abiertos de gobierno*, https://www.gacetaoficial.gob.pa/pdfTemp/28421/GacetaNo_28421_20171207.pdf. [17]

Murtin, F. et al. (2018), "Trust and its determinants: Evidence from the Trustlab experiment", *OECD Statistics Working Papers*, No. 2018/2, OECD Publishing, Paris, https://dx.doi.org/10.1787/869ef2ec-en. [5]

National Law Information Center (2019), *Law by classification*, http://www.law.go.kr/LSW/eng/engLsSc.do?menuId=1&query=%EA%B3%B5%EA%B3%B5%EB%8D%B0%EC%9D%B4%ED%84%B0&x=0&y=0#liBgcolor0. [35]

National Law Information Center (2019), *Law by Classification*, http://www.law.go.kr. [34]

New Zealand Government (2019), *Algorithm Review Underway to Increase Transparency and Accountability*, https://www.data.govt.nz/blog/algorithm-review-underway-to-increase-transparency-and-accountability/. [43]

New Zealand Ministry of Foreign Affairs and Trade (2019), *Christchurch Call*, https://www.christchurchcall.com/call.html. [49]

New Zealand Ministry of Social Development (2019), *Using Personal Information Responsibly*, https://www.msd.govt.nz/about-msd-and-our-work/work-programmes/initiatives/phrae/index.html. [51]

ODI (2017), *Ethical Data Handling*. [22]

OECD (2019), *Digital Government in Chile – Digital Identity*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/9ecba35e-en. [44]

OECD (2019), *Digital Government Review of Panama: Enhancing the Digital Transformation of the Public Sector*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/615a4180-en. [13]

OECD (2019), *Digital Government Review of Sweden: Towards a Data-driven Public Sector*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/4daf932b-en. [10]

OECD (2019), *OECD Glossary of Statistical Terms*, OECD, Paris, https://stats.oecd.org/glossary. [38]

OECD (2017), *Government at a Glance 2017*, OECD Publishing, Paris, https://dx.doi.org/10.1787/gov_glance-2017-en. [2]

OECD (2017), *How's Life? 2017: Measuring Well-being*, OECD Publishing, Paris, https://dx.doi.org/10.1787/how_life-2017-en. [6]

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. [8]

OECD (2016), "Research Ethics and New Forms of Data for Social and Economic Research", *OECD Science, Technology and Industry Policy Papers*, No. 34, OECD Publishing, Paris, https://dx.doi.org/10.1787/5jln7vnpxs32-en. [32]

OECD (forthcoming), *Digital Government Review of Chile*, OECD Publishing, Paris, forthcoming. [21]

OECD (forthcoming), *State of the Art on Emerging Technologies*, OECD, Paris, forthcoming. [40]

OECD/KDI (2018), *Understanding the Drivers of Trust in Government Institutions in Korea*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264308992-en. [7]

Pedley, D. et al. (2018), *Understanding the UK Cybersecurity Skills Labour Market*, Ipsos MORI Social Reearch Institute, https://www.ipsos.com/sites/default/files/ct/publication/documents/2019-01/understanding_the_uk_cyber_security_skills_labour_market.pdf. [48]

Powles, J. and H. Hal (2018), *Response to DeepMind*. [25]

PrivSec Report (2019), *European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows*, Data Protection World Forum Ltd, https://gdpr.report/news/2019/01/24/european-commission-adopts-adequacy-decision-on-japan-creating-the-worlds-largest-area-of-safe-data-flows/. [37]

PrivSec Report (2019), *NHS Patient Data Used by Google Without Consent*, Data Protection World Forum Ltd, https://gdpr.report/news/2019/09/19/privacy-nhs-patient-data-used-by-google-without-consent. [33]

Putman, R., R. Leonardi and R. Nanetti (1993), *Making Democracy Work*, Pinceton Univeristy Press. [3]

Saidot (2019), *A Consortium of Finnish Organisations Seeks for a Shared Way to Proactively Inform Citizens on AI Use*, Saidot, Espoo, Finland, https://www.saidot.ai/post/a-consortium-of-finnish-organisations-seeks-for-a-shared-way-to-proactively-inform-citizens-on-ai-use. [39]

Stats NZ (2019), *Data Ethics Advisory Group*, https://www.data.govt.nz/about/government-chief-data-steward-gcds/data-ethics-advisory-group (accessed on 27 August 2019). [50]

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://doi.org/10.1787/09ab162c-en. [12]

Wagner, B. (2018), *Ethics as an Escape from Regulation: From Ethics-washing to Ethics-shopping?*, Amsterdam University Press, https://www.privacylab.at/wp-content/uploads/2018/07/Ben_Wagner_Ethics-as-an-Escape-from-Regulation_2018_BW9.pdf. [26]

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. [20]

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.

Annex A. Background: OECD work on data-driven public sector

Introduction

The OECD has contributed to the thinking around the role of data in governments, society and the economy. Work from various areas across the OECD helps relevant actors understand the opportunities and challenges presented by recognising the value of data. Box A.2. gives an overview of the OECD work on data. Collectively they form an important body of work that has shaped the conversation about the application of data and allowed for the discussions that led to the development of this report.

The OECD's Going Digital project, initiated in 2017, supports stronger and more inclusive growth from the digital transformation by building a coherent and comprehensive policy approach. It aims to help citizens, governments and businesses shape digital transformation so that it benefits society and leaves no one behind (OECD, 2019[1]). Digital transformation impacts every aspect of our lives; while there are opportunities for this to improve lives, there is also a risk of it disrupting things in ways that negatively impact on people's well-being.

The *OECD Recommendation of the Council on Digital Government Strategies* (OECD, 2014[2]) provides the basis for governments to consider their role in creating the strategic conditions for a digital by design and data-driven culture. These conditions not only have an impact on ministerial institutions and the "business of government", but should also foster effective delivery throughout the public sector and its agencies including providers of health, education, and other public goods and services. Principle 3 of the Recommendation focuses on data, and specifically the need for supportive frameworks to encourage the re-use of data and build the foundations for unlocking the value of raw and isolated data in delivering 21st century digital government (Box A.1.)

Box A.1. OECD Recommendation of the Council on Digital Government Strategies: Principle 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 reuse 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 reuse, and the possibility for non-governmental actors to reuse and supplement data with a view to maximising public economic and social value).

Source: OECD (2014[2]), Recommendation of the Council on Digital Government Strategies, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406.

The crosscutting nature of the role of data throughout society highlights the value of collaboration within the OECD. The OECD Secretariat brings together the ecosystem of actors engaged in the digital economy, open data and open science policy areas at the country level to better understand how the fostering of improved access and sharing of data can contribute to better governance and public value creation.

This report draws on cross-directorate work within the OECD, including the OECD Project on Enhancing Access to and Sharing of Data, led by the OECD Directorate for Public Governance and the Directorate for Science, Technology and Innovation, through their relevant committees – the Public Governance Committee; the Committee on Digital Economy Policy; and the Committee for Scientific and Technological Policy.

Other OECD Recommendations, such as the *OECD Recommendation of the Council concerning Access to Research Data from Public Funding* (OECD, 2006[3]), the *OECD Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information* (OECD, 2008[4]) address data access and sharing, and provide guidance and best practices.

OECD work on public sector data

The OECD Directorate for Public Governance, has worked with OECD member and partner countries to:

- Support governments in how the use of data can transform the public sector and issues of public governance through the data-driven public sector work stream initiated at the request of delegates at the 2015 meeting of the OECD Working Party of Senior Digital Government Officials (E-Leaders). This includes the work of the E-Leaders Thematic Group on a Data-driven Public Sector; the working paper "A data-driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance" (Ubaldi, van Ooijen and Welby, 2019[5]); and the analysis from various Digital Government Reviews. However, more critically it reflects the specific experiences of the six member countries (Denmark, Ireland, Korea, Portugal, Sweden and the United Kingdom) that contributed to a comparative study of their own experiences. The output of the initial comparative research was discussed during the 2018 meeting of the OECD Working Party of Senior Digital Government Officials (E-Leaders) in Seoul, Korea.
- Assess how data governance models are implemented, and integrated, within the framework of broader public sector digitalisation efforts, including digital government and government data policies and initiatives.
- Analyse how the components of data governance models (i.e. leadership; stewardship; and policies, rules, standards and data interoperability) are deployed within public sector organisations and across different policy sectors, and provide the ground for greater proactive, collaborative and open policy approaches (e.g. by opening up government data and using it for the joint design and delivery of public services).
- Promote the definition, implementation, impact and sustainability of open government data (OGD) policies (OECD, 2018[6])
- Explore the state of the art in emerging technologies including artificial intelligence and blockchain through the work of the E-Leaders Thematic Group on Emerging Technologies (Ubaldi et al., 2019[7]) and the OECD's Observatory of Public Sector Innovation (OECD Observatory of Public Sector Innovation, 2019[8]; OECD, 2018[9])
- Understand the drivers of trust in government institutions and use guidelines on measuring trust (OECD, 2018[10]; 2017[11]).

The OECD's work on public sector data draws upon the expertise of the Directorate for Public Governance through different work streams, namely:

- national reviews on the digital transformation of the public sector addressing public sector data governance [see for instance (OECD, 2017[12]; 2018[13]; 2019[14]; 2019[15]; 2019[16]; 2019[17])], OGD [see for instance (OECD, 2016[18]; 2018[19])], and digital government as a whole [see (OECD, 2018[20]; 2016[21])]
- Recent and previous research work including the OECD Comparative Study on Data-driven public sector (unpublished); and working papers on data-driven public sector (Ubaldi, van Ooijen and Welby, 2019[5]), on well-being (Welby, 2019[22]), and OGD (Ubaldi, 2013[23]).
- Comparative analytical work on OGD, including the 2018 OECD Open Government Data Report (2018[6]); the OECD Open, Useful and Re-usable Data (OURdata) Index; and OECD Compendium of good practices on the use of open data for anti-corruption (OECD, 2017[24])
- Measurement work on OGD, namely the OECD Open Government Data Survey and the 2014, 2016 and 2019 (forthcoming) editions of the OECD Open, Useful and Re-usable (OURdata Index) [see (OECD, 2015[25]; 2017[26]; 2017[27])]; and on digital government, namely the Digital Government Survey 1.0 (2018/19).

These work streams are under the auspices of the OECD Working Party of Senior Digital Government Officials (E-leaders) and the Expert Group on Open Government Data, and are aligned to the principles of the OECD Recommendation of the Council on Digital Government Strategies (OECD, 2014[2]).

Box A.2. A brief overview of the OECD work on data

Recommendations

- OECD *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD, 2013[28]) under the responsibility of the Committee on Digital Economy Policy
- OECD *Recommendation of the Council concerning Access to Research Data from Public Funding* (OECD, 2006[3]) under the responsibility of the Committee for Scientific and Technological Policy
- OECD *Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information* (OECD, 2008[4]) under the responsibility of the Committee on Digital Economy Policy
- OECD *Recommendation of the Council on Digital Government Strategies* (OECD, 2014[2]) under the responsibility of the Public Governance Committee
- OECD *Recommendation on Enhanced Access to and Sharing of Data* is being jointly developed by these three committees to develop a global view of the topic.

Working papers

- "Open government data: Towards empirical analysis of open government data initiatives" (Ubaldi, 2013[23])
- "A data-driven public sector" (Ubaldi, van Ooijen and Welby, 2019[5])
- "Using digital technologies to improve the design and enforcement of public policies" (OECD, 2019[29])

Reports

- *Data-Driven Innovation: Big Data for Growth and Well-Being* (OECD, 2015[30])
- *Open Government Data Report: Enhancing Policy Maturity for Sustainable Impact* (OECD, 2018[6])

Reviews

- Open Government Data Review of Poland (OECD, 2015[31])
- Open Government Data Review of Mexico (OECD, 2016[18]) and its follow up project (OECD, 2018[19])
- Digital Government Review of Norway (OECD, 2017[12])
- Digital Government Review of Sweden (OECD, 2019[14])
- Digital Government Review of Argentina (OECD, 2019[15])
- Digital Government Review of Peru (OECD, 2019[16])
- Digital Government Review of Panama (OECD, 2019[17])

Indicators

- Open, Useful and Reusable Government Data Index (OURdata Index) in Government at a Glance 2017 (OECD, 2017[26])
- Digital government indicators (forthcoming)

Working parties and expert groups

- OECD Working Party of Senior Digital Government Officials (E-Leaders), incorporating a Thematic Group on the Data-driven Public Sector
- OECD Working Party on Security and Privacy in the Digital Economy
- OECD Working Party on Data Governance and Privacy in the Digital Economy
- OECD Expert Group Meeting on Open Government Data

References

OECD (2019), *Digital Government in Peru: Working Closely with Citizens*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/0c1eb85b-en. [16]

OECD (2019), *Digital Government Review of Argentina: Accelerating the Digitalisation of the Public Sector*, OECD Publishing, Paris, https://www.oecd-ilibrary.org/governance/digital-government-review-of-colombia_9789264291867-en (accessed on 24 June 2019). [15]

OECD (2019), *Digital Government Review of Panama: Enhancing the Digital Transformation of the Public Sector*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/615a4180-en. [17]

OECD (2019), *Digital Government Review of Sweden : Towards a Data-driven Public Sector*, OECD Publishing, Paris, https://doi.org/10.1787/24131962. [14]

OECD (2019), *Going Digital: Shaping Policies, Improving Lives*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264312012-en. [1]

OECD (2019), "Using digital technologies to improve the design and enforcement of public policies", *OECD Digital Economy Papers*, No. 274, OECD Publishing, Paris, https://dx.doi.org/10.1787/99b9ba70-en. [29]

OECD (2018), *Digital Government Review of Brazil: Towards the Digital Transformation of the Public Sector*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264307636-en. [20]

OECD (2018), *Digital Government Review of Colombia: Towards a Citizen-Driven Public Sector*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264291867-en. [13]

OECD (2018), *OECD Blockchain Primer*, http://www.oecd.org/finance/OECD-Blockchain-Primer.pdf. [9]

OECD (2018), *Open Government Data in Mexico: The Way Forward*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264297944-en. [19]

OECD (2018), *Open Government Data Report: Enhancing Policy Maturity for Sustainable Impact*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264305847-en. [6]

OECD (2018), *Understanding the Drivers of trust in Government Institutions in Korea*. [10]

OECD (2017), *Compendium of good practices on the use of open data for Anti-corruption: Towards data-driven public sector integrity and civic auditing*, OECD Publishing, Paris, http://www.oecd.org/gov/digital-government/g20-oecd-compendium.pdf (accessed on 5 September 2018). [24]

OECD (2017), *Digital Government Review of Norway: Boosting the Digital Transformation of the Public Sector*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264279742-en. [12]

OECD (2017), *Government at a Glance 2017*, OECD Publishing, Paris, http://dx.doi.org/10.1787/22214399. [26]

OECD (2017), *Government at a Glance: Latin America and the Caribbean 2017*, OECD Publishing, Paris, https://www.oecd-ilibrary.org/docserver/9789264265554-en.pdf?expires=1535456470&id=id&accname=ocid84004878&checksum=9E33F8A1DA493CE7E85B886BFA7B963E (accessed on 28 August 2018). [27]

OECD (2017), *OECD Guidelines on measuring trust*. [11]

OECD (2016), *Digital government in Chile: Strengthening the institutional and governance framework.*, OECD Publishing, Paris, https://doi.org/10.1787/24131962. [21]

OECD (2016), *Open Government Data Review of Mexico: Data Reuse for Public Sector Impact and Innovation*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264259270-en. [18]

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264229358-en. [30]

OECD (2015), *Government at a Glance 2015*, OECD Publishing, Paris, https://dx.doi.org/10.1787/gov_glance-2015-en. [25]

OECD (2015), *Open Government Data Review of Poland: Unlocking the Value of Government Data*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264241787-en. [31]

OECD (2014), *Recommendation of the Council on Digital Government Strategies, OECD/LEGAL/0406*, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406. [2]

OECD (2013), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. [28]

OECD (2008), *Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information, OECD/LEGAL/0362*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0362 (accessed on 24 July 2019). [4]

OECD (2006), *Recommendation of the Council concerning Access to Research Data from Public Funding, OECD/LEGAL/0347*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0347. [3]

OECD Observatory of Public Sector Innovation (2019), *Hello, World: Artificial Intelligence and its Use in the Public Sector (draft)*, OECD Observatory of Public Sector Innovation, Paris, https://oecd-opsi.org/projects/ai. [8]

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, https://dx.doi.org/10.1787/5k46bj4f03s7-en. [23]

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, Paris. [7]

Ubaldi, B., C. van Ooijen 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, http://dx.doi.org/10.1787/09ab162c-en. [5]

Welby, B. (2019), "The impact of Digital Government on citizen well-being", *OECD Working Papers on Public Governance*, No. 32, OECD, Paris. [22]

Annex B. Data-driven integrity

Introduction

Applying the concepts of a data-driven public sector to integrity actors

Data are a driver of many initiatives to prevent fraud or corruption, such as the use of data to assess risks, automate control activities, or manage asset declarations and conflicts of interests. This case study explores the application of a data-driven public sector (DDPS) framework to integrity actors in government. It considers how and to what extent the different elements of a DDPS – data governance, data for creating value in public service delivery and data for promoting citizen's trust – are applicable to the policies, practices and tools of governmental integrity actors. It emphasises both opportunities and limitations for applying the DDPS framework, taking into account the mandates of integrity actors vis-à-vis those responsible for defining and executing digital government strategies.

Conversely, the case study highlights ways that the DDPS framework can benefit from the expertise and data issues facing integrity actors. Integrity actors have subject matter expertise that can be a useful input for key elements of the DDPS, such as data privacy and ethics. In addition, integrity actors are also key users of data from across government and sectors. Their use of data for preventing and detecting fraud affords them a unique perspective to support refinements to the formulation and implementation of policies, frameworks and guidance for a DDPS.

The term "data-driven" is inherent in the DDPS framework, and therefore is used throughout the case study. Nonetheless, the idea that integrity actors can also benefit from simply being "data-informed" is worth noting upfront. Implicit in this idea is the notion that data are often one of many critical inputs for the work of integrity actors, which also relies on human elements, such as sound judgement, professional scepticism and expertise.

Who are public sector "integrity actors" in this case study?

This case study refers generally to integrity actors as the entities or individuals responsible for designing, implementing or overseeing policies and practices to promote integrity and prevent fraud or corruption in the public sector. The definition is broad to accommodate a range of institutions or individuals that could benefit from using data for the said purpose. For instance, integrity actors in government can include ethics offices, anti-corruption bodies, supreme audit institutions, ombudsmen, and internal audit or control functions within line ministries. They can also be law enforcement agencies, prosecutor's offices, the courts or other institutions with judicial or punitive mandates, all of which can advance and support the use of data to prevent and detect corruption. In addition, integrity actors can be individuals, such as managers responsible for controls and risk assessments as part of service delivery and operational activities.

This case study does not attempt to capture the experiences of all the institutions or individuals that could be considered integrity actors. This inclusive, broad definition of integrity actors works for the purposes of this case study because the primary focus is assessing the application of the principles and practices of the DDPS framework, and use of data more specifically, for preventing and detecting fraud, corruption,

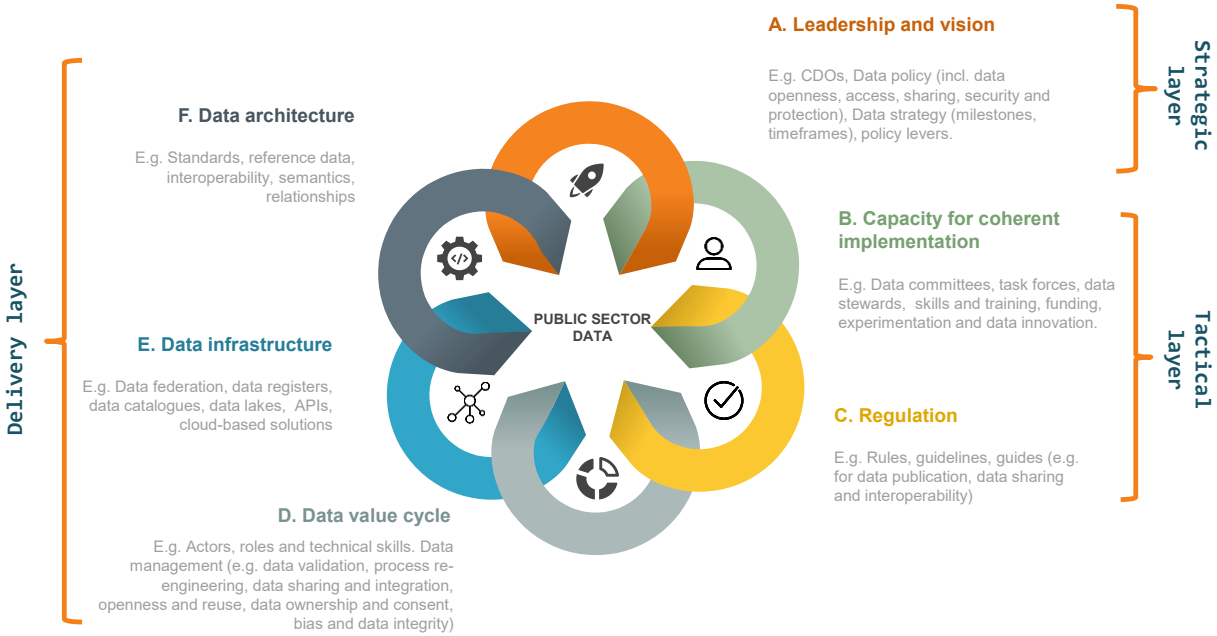
waste and abuse. As such, this broad definition provides some flexibility for exploring the practices and examples that could be transferable across institutions and sectors.

Data governance and preconditions for effective use of data by integrity actors

Effective data governance is a critical precondition for data-driven approaches to prevent and detect fraud or corruption. For instance, Korea's Bid Rigging Indicator Analysis System (BRIAS) facilitates quantitative assessments of collusion in public procurement (OECD, 2017[1]). The ability of BRIAS to facilitate electronic transfers of bidding information from hundreds of government institutions, and to convert those data into corruption indicators, relies on a robust data architecture and infrastructure. In addition to these elements of data governance, how governments manage the data value cycle – collecting, generating, storing, securing and processing of data – has direct implications for the ability of integrity actors to prevent and detect fraud and corruption. For example, data interoperability across government is essential for auditors or anti-corruption bodies to carry out data matching using databases maintained by different government entities in order to identify fraud, waste and abuse. Figure B.1 summarises the various elements of data governance, many of which are preconditions for integrity actors to create value from data.

Figure B.1 shows the key elements for which centre-of-government (CoG) ministries are responsible in order to strengthen data governance across government and enhance a DDPS. Nonetheless, integrity actors are prosumers of data – both creators and users – and can offer unique experiences and insights to help the CoG shape broader digital government strategies. This has been the case in many countries for advancing the open data movement. For instance, in Indonesia, the Corruption and Eradication Commission played a critical role in facilitating the communication and co-ordination among stakeholders not only to implement anti-corruption policy reforms, but also to work with the Office of the President to advance the open data agenda. In Argentina, the Anti-Corruption Office contributed to the work of the Chief of Cabinet Office and the then Ministry of Modernisation to develop a decree on open data, which mandated the publication of key datasets and set timelines for ministries to develop open data plans (OECD, 2019[2]).

Figure B.1. Data governance in the public sector



Source: OECD (2019[2]), *Digital Government Review of Argentina: Accelerating the Digitalisation of the Public Sector*, https://doi.org/10.1787/354732cc-en.

Integrity actors can be useful contributors to a DDPS beyond the open data context. They are often at the frontlines of inter-ministerial or inter-sectoral discussions about the technical and regulatory challenges for using data while balancing competing policy priorities, such as privacy issues and use of personally identifiable information. For example, the supreme audit institution of the United States, the Government Accountability Office, has organised several multi-stakeholder forums and communities of practices with government, civil society and the private sector to explore ways the government can maximise the benefits of data and limit possible drawbacks. One forum brought together experts from across sectors to discuss the use of data analytics to address fraud and improper payments, including identifying ways to improve collaboration, such as overcoming legal and data-sharing barriers. Supreme audit institutions, like other integrity actors, have a whole-of-government view based on their work and use of government-wide data sources that can help the CoG shape and refine digital government strategies and policies.

By contributing to the national dialogue on digital government strategies, integrity actors can also help to advance their own agendas and address their unique challenges. For example, data interoperability and data-sharing issues can be especially pronounced in the integrity space, as illustrated in Box B.1, since integrity actors often rely on multiple data registries and databases across government and sectors to identify risks and conduct investigations. Ultimately, by improving data governance and promoting consistency and coherence across institutions, governments can help integrity actors spend more time and resources (re)using data, and less time and fewer resources managing data governance issues.

Box B.1. Challenges of interoperability in customs in the European Union

In May 2016, the European Commission set up a high-level expert group on information systems and interoperability. In its final report in May 2017, the high-level expert group highlighted, among others, the potential added value of interoperability between the customs and Justice and Home Affairs (JHA) systems. Improving interoperability between the systems of the two authorities could enable sharing of real-time information in a systematic and automated way. The high-level expert group focused on the reality that customs and JHA information systems were not interoperable, leading to blind spots for both JHA and custom authorities. For the custom authorities, the systems are a critical tool for managing risk-based controls at the external borders, which includes detecting and preventing the trafficking of goods posing security or safety risks.

To address this challenge, the commission established an expert group of practitioners with operational knowledge of border management, customs and security. The group analysed the data that could be compatible by mapping the different systems of customs authorities and the JHA in the area of security, border and migration management. The mapping informed a feasibility study on the specific interoperability efforts that could enhance the management of security risks.

The work also supported the group's efforts to inform policy makers on their specific opportunities and challenges related to interoperability. For example, to strengthen investigative capacity, the experts determined that law enforcement authorities should have direct access to a centralised Advance Cargo Information System (ICS2). From 2021, this system will replace the existing system (ICS) for collecting electronic information on goods coming into or through the European Union customs territory.

Source: European Commission (2018[3]), Interoperability of Security and Border Management Systems with Customs Systems: Assessment Report of the Practitioners, www.statewatch.org/news/2019/mar/eu-council-interoperability-customs-5574-19.pdf.

Data for creating value in the work of integrity actors

The DDPS framework highlights three main areas of opportunity for a data-driven public sector: 1) anticipatory governance; 2) design and delivery of services; and 3) performance management. This section

explores the relevance of these areas for integrity actors and the use of data to prevent and detect fraud and corruption. Overall, these three areas provide a useful framework for understanding how data can support decision making and the activities of integrity actors, although some elements, such as performance management, pose challenges for integrity actors given the hidden nature of fraud and corruption. In this context, prevention refers to ex ante approaches for avoiding fraud and corruption, or lessening their impact and likelihood. Detection is an ex post activity for identifying fraud or corruption that has already occurred. This distinction helps to understand the value of data-driven approaches, as well as their limitations.

Data for anticipating governance

Anticipatory governance in the DDPS framework generally refers to the use of data as part of a systematic effort to take into account a possible future to take decisions in the present. The framework focuses on two aspects of anticipatory governance: forecasting and foresight. According to the DDPS framework, data-driven "foresight" activities take into account possible future outcomes, without necessarily predicting specific cases of fraud and corruption based on past experiences. The DDPS framework defines forecasting as the use of data to "predict" the most likely developments and outcomes (van Ooijen, Ubaldi and Welby, 2019[4]). The distinction between the two in the integrity context is subtle. In general, activities to prevent fraud or corruption reflect the DDPS framework's definition of foresight, while detection activities have a conceptual link to forecasting. Nonetheless, some activities of integrity actors, like risk assessments, can serve both purposes.

Data-driven risk assessments can be one example of using data for both foresight and forecasting. Data can support quantitative assessments of the likelihood, impact and velocity of risks, and inform the identification of high-risk organisations or individuals that are susceptible to fraud or corruption (OECD, 2019[5]). Risk assessments can be carried out manually (i.e. with experts) or automated, such as the case of the Arachne tool for the European Union (see Box B.2). Insights gleaned from the data can then be used to pre-emptively prevent fraud or corruption by adapting controls before expenditures are made. In this sense, data facilitates the foresight that ultimately shines a light on the various vulnerabilities in the control environment, without necessarily targeting specific cases or individuals. This is meant to avoid the classic "pay and chase" model, whereby a government entity makes an improper payment and then spends additional taxpayer resources to identify, investigate and possibly recoup those payments.

Box B.2. Use of Arachne in the European Union

The European Commission encourages the use of data analytics to enrich the risk assessment process, and in particular, the use of Arachne, a web-based tool with data on contractors, contracts, beneficiaries and projects (European Commission, 20014[6]). Arachne became operational in 2013 as a tool to support authorities of EU member states to identify and prioritise fraud risks, conflicts of interest and irregularities in European Structural and Investment Funds. Data sources for Arachne include data from managing authorities as well as external databases (e.g. ORBIS and World Compliance). In December 2018, according to the European Commission, 21 member states used Arachne for 165 operational programmes, which accounted for 54% of all EU cohesion funding for 2014 20 (excluding the European Territorial Co-operation objective of the European Regional Development Fund) (European Court of Auditors, 2019[7]).

Arachne helps managing authorities to identify high-risk projects, contracts, contractors and beneficiaries with the help of over 100 risk indicators linked to 7 risk categories. Those risk categories include procurement, contract management, eligibility, performance, concentration, reasonability and reputational, and fraud alerts. The specific types of fraud risks and red flags that Arachne supports include:

- financial: overall financial performance of beneficiaries, contractors/suppliers and subcontractors, based on financial reporting data
- relationship: the existence of relationships between beneficiaries and contractors/suppliers or sub-contractors and their respective personnel
- reputation: involvement in activities (such as bankruptcies) that could possibly result in reputational damages
- sanctions: identification of beneficiaries, contractors/suppliers, subcontractors or their respective personnel, blacklisted by appearing on any type of sanctions list
- change: any type of changes to the company structure
- procurement: the lead time between the publication of the tender notice and contract signature
- contract management: contract addenda cost (total) for the project and actual project cost
- eligibility: project costs outside the eligibility period, such as before the start date or after the end date
- performance: number of people trained or to be trained
- concentration: beneficiaries involved in multiple projects
- other checks: European Commission financial assistance and total project cost.

The OECD supported the government of the Slovak Republic to improve its fraud and corruption risk management in European Structural and Investment Funds, which Included an analysis of its use of Arachne. Managing authorities in the Slovak Republic supplement Arachne with several other databases, including the Information Technology Management System, the Irregularity Management System, the Early Detection and Exclusion System, company registers, and procurement databases. Managing authorities said that the most commonly applied data analytics techniques they use, with the support of these systems, are traditional rules-based detection and descriptive tests, such as data matching and data mining. The success of Arachne relies in large part on the ability of these systems to communicate with each other, and on the input of data by managing authorities for calculating risk indicators.

Source: OECD (2019), Tackling Fraud and Corruption Risks in the Slovak Republic: A Strategy with Key Actions for the European Structural and Investment Funds, OECD Public Governance Reviews, Source: OECD (2019), Tackling Fraud and Corruption Risks in the Slovak Republic: A Strategy with Key Actions for the European Structural and Investment Funds, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/6b8da11a-en.

Fraud and corruption are deliberate and non-random, therefore traditional audit methods involving the use of statistical sampling can be ineffective for identifying corruption or fraud (Dilla and Raschke, 2015[6]). Data can support methodologies for forecasting, or "predicting", where fraud or corruption could have occurred, or is ongoing, in a particular programme or transactions. For instance, auditors and investigators routinely make use of data analytic techniques, such as data mining, to uncover fraudulent activities. Forecasting in this sense, unlike foresight, is not necessarily aimed at taking preventive actions (e.g. adapting controls) based on possible outcomes, but rather to target audit or investigative resources towards specific instances of possible fraud or corruption.

Examples of data mining are common for detecting collusion in public procurement or conflicts of interest; however, there are other applications. For example, in the People's Republic of China, the supreme audit institution used data-mining methods to analyse data and geographic information from across government ministries to assess compliance with environmental regulations. The analysis showed that smaller factories had more compliance problems than larger ones in certain regions, and that specific factories continued production at night or surreptitiously to avoid emissions controls. This finding led to more targeted oversight and reforms (OECD, 2019[7]).

In addition to data mining, data-driven predictive audits can serve a similar purpose to support programme objectives. For example, such audits can help to judge the probability of default of government loans or the likelihood that certain transactions on government credit cards or applications for government assistance are indicative of fraud. A DDPS – with robust data governance, in particular – promotes and facilitates such efforts to forecast specific problem areas, and help integrity actors to take advantage of administrative data, as well as other types of data.

As discussed below, some integrity actors (e.g. supreme audit institutions or sector-specific integrity units) attempt to conduct government-wide analysis about the extent of fraud and the financial losses incurred by taxpayers and the government. This analysis can help policy makers and line ministries to take decisions about legal and policy reforms, resource allocation, and co-ordination strategies, for instance. Moreover, data (e.g. "big data") can provide insights into the future needs of society, which in turn can inform the potential strategies and foresight activities of integrity actors. For example, data on climate change can inform anti-fraud strategies and targeting of possible hotspots for delivering disaster assistance, and data on the changing demographics of populations can help shape fraud and corruption controls when distributing social benefits, pensions and healthcare subsidies.

While integrity actors can support anticipatory governance, by and large, using data for this purpose is aspirational and evidence of "what works" is either anecdotal or raises questions for further research. For instance, in its flagship report, the Association of Certified Fraud Examiners (ACFE) reported that the use of "proactive data monitoring and analysis" and surprise audits were associated with a more than 50% reduction in fraud losses, based on a median loss calculation before and after controls (ACFE, 2018[8]). While interesting to note, the ACFE's survey does not distinguish between private sector and government sectors, and the methodology for the calculation is unclear. Perhaps as a telling sign for the quality of data in or provided by government, the 2018 "Government Edition" of the ACFE's report does not provide the same indicator for proactive data monitoring and analysis (ACFE, 2018[9]). In reality, data for anticipatory governance in the integrity context is a maturing area. As discussed, data governance at a government-wide level is often a hindrance, which has implications for practical issues such as skills, co-ordination challenges for sharing data, time and resources.

Data for enhancing integrity activities and engaging stakeholders

The DDPS highlights the ability of data to improve public service delivery and engage civil society to promote trust and participation in government (van Ooijen, Ubaldi and Welby, 2019[4]). This concept is uniquely reflected in the work of integrity actors. The service integrity actors provide links directly with broader principles of governance, such as ensuring the accountability of managers. Their work facilitates citizens' trust in government, and as interpreters of data, integrity actors can shine a light on governance problems for policy makers, line ministries and the public at large. In addition to data for anticipatory governance (i.e. foresight and forecasting), Table B.1 illustrates some of the everyday key questions that a DDPS and data can help integrity actors address.

Table B.1. Key questions that data can address

	Hindsight	Insight	Forecasting/foresight
Information	What happened? (reporting)	What is happening now? (alerts)	What will happen? (extrapolation)
Knowledge	How and why did it happen? (modelling, experimental design)	What's the next best action? (recommendation)	What's the best/worst thing that can happen? (prediction, optimisation, simulation)

Source: OECD (2019[5]), Analytics for Integrity: Data-Driven Approaches for Enhancing Corruption and Fraud Risk Assessments, www.oecd.org/gov/ethics/analytics-for-integrity.pdf; adapted from Davenport, T.H., J.G. Harris and R. Morison (2010[10]), Analytics at Work: Smarter Decisions, Better Results.

To answer these questions, integrity actors rely on a variety of data sources and formats (e.g. data that are open, big, administrative, structured, unstructured, etc.). Some examples of data sources that can support the work of integrity actors to answer the questions above, particularly to identify and analyse integrity risks, including the following:

- employee, household or business surveys;
- other survey data, such as user surveys, or polls from local research institutions;
- data from public registries (e.g. law enforcement, audit institutions, national statistics office);
- published research documents from national or international organisations or academia (e.g. articles, reports, working papers, political economy analysis) ;
- commissioned research;
- indicators from international organisations or research institutions;
- interviews or focus groups with relevant stakeholders; and
- risk assessments conducted by ministries or other government entities for their own programmes (OECD, forthcoming[11]).

The Office of the Auditor General of Western Australia (OAG-WA) illustrates the use of transactional data and the value of using data analytics to provide both hindsight and foresight to improve public financial management. The OAG-WA analysed payroll data to identify possible fraud, errors and omissions. Data matching and data interrogation techniques allowed auditors to analyse 4 million transactions from 2014 to 2015 totalling over EUR 7.5 billion from 12 different government agencies. Auditors did not find evidence of fraud, but they found overpayments and a need for improved controls in half of the agencies tested (OAG-WA, 2016[12]). The data governance in the local government where the OAG-WA operates, along with its own capacity and skills, allowed the OAG-WA to use data analytics in this way and recommend solutions to pressing governance and control issues. Other countries have similar successful experiences of using data to prevent and detect improper payments, and more generally, to promote accountability (see Box B.3 for an example from Brazil).

Box B.3. Data-driven oversight of Brazil's supreme audit institution

Better strategies, capacity, skills and tools for using data has allowed supreme audit institutions to perform increasingly innovative oversight activities over the last decade. The following examples, selected by Brazil's supreme audit institution, illustrate how data can be used to detect fraud and foster a more efficient and accountable public administration.

A data-mining system to detect fraud in the Brazilian public healthcare system

The large size of the healthcare sector and the amount of money it represents make it an attractive target for fraud. Using several databases, Brazil's supreme audit institution, the Tribunal de Contas da União, uses the InfoSAS system to spot statistical anomalies in the services delivered by SUS, Brazil's publicly funded healthcare system.

While individually analysing each of the 5 000 medical targets and approximately 6 000 providers to check for anomalies would require extracting billions of factsheets through the system, InfoSAS uses various algorithms to detect discrepancies, producing scores that can sort and prioritise factsheets. It detects sudden variations in a provider's production and assigns a discrepancy score to each institution, which draws the analyst's attention to carry out more in-depth analyses.

While statistical discrepancies should be considered cautiously due to the existence of various explanations, their use represents a step forward in modernising selection processes for audit and control items, allowing the Tribunal de Contas da União to detect fraud more efficiently.

Geo-technologies and the monitoring of Sustainable Development Goals by supreme audit institutions

Recent resolutions of the UN General Assembly emphasise the key role of supreme audit institutions and of the International Organization of Supreme Audit Institutions (INTOSAI) in meeting Sustainable Development Goals: supreme audit institutions perform an important role in promoting the efficiency, accountability, effectiveness and transparency of the public administration, fostering national development around the Sustainable Development Goals. The use of geospatial data being one of the initiatives proposed by the UN, the International Standards of Supreme Audit Institutions (ISSAIs) has described the possible applications of geo-technologies to several audit phases and issued guidance on the use of geographic information systems.

In particular, spatial data sources may be exceptionally useful to supreme audit institutions when checking environmental issues with clear geographic aspects, such as environmental protection areas or polluted areas. Geospatial data are also useful to select samples from different sites, find high-risk areas and standards in data, which would not be possible without this spatial component. Supreme audit institutions may also use spatial data to present audit results, making them more tangible.

Source: TCU (2016[13]), "InfoSAS: A data mining system for production control of SUS", https://revista.tcu.gov.br/ojs/index.php/RTCU/issue/view/68/102; TCU (2016[14]), "Geotechnologies and monitoring of Sustainable Development Goals by supreme audit institutions",https://revista.tcu.gov.br/ojs/index.php/RTCU/issue/view/68/102.

The work of some integrity actors is directly aligned with an institution. For instance, internal audit functions are meant to support organisational goals through assurance and control of expenditures, thereby ensuring that taxpayer funds are used for their intended purposes. Ethics offices have a similar arrangement, as they are embedded within an institution's organisational structure. Data can help these actors to mainstream their activities into the internal governance system. This can include reducing uncertainties in managerial decision making through data-driven risk assessments, or using data analytics to pull information from across an organisation to combat silos and strengthen entity-wide knowledge and information. The preconditions for effective data governance at this level are similar to those across government. Institutional leadership, capacity, skills and a willingness to experiment at an institutional level are all critical factors for keeping pace with a data-driven environment (OECD, 2019[7]).

The OECD's work to support public sector integrity in a number of areas, from managing fraud risk in European Structural Investment Funds to preventing fraud and corruption in government in Latin America, Asia, and the Middle East and North Africa, demonstrates a wide-ranging need for improving "the basics" for data-driven approaches. In the Middle East and North Africa, for instance, the OECD surveyed seven economies (Egypt, Jordan, Lebanon, Morocco, Oman, the Palestinian Authority and Tunisia) and identified common government-wide and institutional challenges for using data to support integrity and anti-corruption work. This included typical challenges of poor data strategies and data infrastructure across government, as well as specific issues like the need for tailoring interventions to build data skills based on job roles (OECD, 2017[15]).

In addition, responses from a non-generalisable survey of the OECD's Auditors Alliance suggested a heavy reliance on Microsoft Excel and the need to improve simple data extraction tools to support data management and pre-analytical processing of data. Respondents also reported a limited use of automated data extraction tools, which has the potential to become a more significant issue in the future as financial data and digitalisation of "evidence" across government accelerates (e.g. financial transactions, purchase orders, signatures, invoices, etc.). This underscores the importance of a DDPS to not only advance the delivery and strategic layers of data governance, but also the tactical layer, in particular, developing capacities for coherent implementation. The challenges are not just technical. In the same survey, nearly a quarter of respondents highlighted budget limitations as the top challenge for making better use of data and computer-assisted auditing techniques (OECD, 2019[7]).

In the integrity context, the benefits of using data often focus on identifying areas of high risks, yet data also offer value for identifying and adapting controls related to low-risk areas. Traditional risk treatments generally fall into four main categories, depending on the level of risk. Terms vary for the treatments, but they typically reflect the ideas of risk mitigation, avoidance, transfer and acceptance. Acceptance is particularly relevant for risks that are perceived as low likelihood and low impact. Fraud and corruption prevention strategies are calibrated to minimise controls of low risks. This can have practical effects on individuals and their experiences with government services. For instance, for social benefit programmes, data can reveal which claims and recipients pose a greater fraud risk, as well as claims and recipients who are minimal risks.

Through data-informed risk management, a DDPS approach can reduce checks on recipients who have a good record of compliance and a low risk of engaging in fraud. In Denmark, the government entity that manages social security and pension payments (Udbetaling Danmark) noted that the increased use of data for preventing fraud and error comes with other benefits for legitimate claimants, such as streamlining the administration of social benefits across branches of the entity (European Commission, 2015[15]). In this sense, data-driven fraud control is not about targeting bad actors, but serving the good ones well – a notion reflected in the fraud control strategy of the Irish Department of Social Protection, which has the stated goal of ensuring "the right person is paid the right amount of money at the right time" (European Commission, 2015[15]).

So far, the discussion has focused on the pre-analytical and analytical processes, tools, benefits and challenges in the integrity context. However, public value of data does not just come from analysing the data, but from conveying the findings in a way that leads to actionable insights and solutions. Methods such as interactive data visualisation help make conceptual issues real in ways that can be presented for different audiences and that provide specific entry points to engage stakeholders in contributing potential solutions (van Ooijen, Ubaldi and Welby, 2019[4]). Data visualisations and data dashboards are also critical tools for interpreting risks, and creating actionable insights for internal and external stakeholders, as illustrated in Box B.4. Data visualisation is the "visual representation of statistical and other types of numeric and non-numeric data through the use of static or interactive pictures and graphics" (Gatto, 2015[16]). In essence, in the context of integrity actors and applications of anticipatory governance, data visualisation can be a communication tool for sharing results, such as the outcomes of risk assessments. In this example, the results of the analysis should facilitate a common understanding of risks, while complementing perceptions with evidence and countering biases inherent in qualitative approaches. Data visualisations can help promote this value proposition.

Box B.4. The Data Dashboard of Queensland's Crime and Corruption Commission

The Crime and Corruption Commission, in its mission to combat and reduce the incidence of major crime and corruption in the public sector in Queensland (Australia), receives complaints about corrupt conduct from members of the public and public sector agencies.

In the interests of transparency and to assist public sector agencies to better understand corruption risk, the Crime and Corruption Commission created a data dashboard through which ordinary citizens can learn about the number and types of allegations as well as the institutions and activities related to the alleged cases of corruption between 1 July 2015 and 31 March 2019.

By providing a user-friendly data-visualisation tool, downloadable raw data, help resources and a tutorial video, the commission empowers citizens: using this anonymised "barometer" of corrupt conduct as a first step, citizens can request specific information on a case-by-case basis and hold the Crime and Corruption Commission accountable if the allegations do not seem to be followed by actions. This

transparency tool also allows citizens to better understand the data used by this integrity body without disclosing identifiable information.

Source: Crime and Corruption Commission (2019[17]), Corruption Allegations Data Dashboard,. www.ccc.qld.gov.au/corruption-prevention/corruption-allegations-data-dashboard/corruption-allegations-data-dashboard-about

Data for performance management

The DDPS framework identifies how data can support performance management, including more efficient use of resources, evaluation and continuous improvement. For integrity actors, this particular aspect of the DDPS framework poses challenges because of difficulties in measuring the impact of prevention measures. This issue is not simply a matter of improving data governance, such as data access, quality or interoperability; the issue is a measurement challenge, which in the best of cases relies on statistical models to determine fraud rates and create baselines. Without such baselines, it is difficult for institutions to measure the efficacy of control activities. As a result, assessment of the effectiveness of prevention and detection activities are often anecdotal, or captured during the course of control planning processes, such as risk assessments.

While a baseline for the extent of fraud and corruption is difficult to establish, countries are exploring ways to make use of the data they have to paint a "good enough" picture that can still be useful for policy making. Examples are often sector-specific, particularly in health or social benefit programmes, focus on detected fraud or corruption, or capture bigger concepts like improper payments. For instance, in 2014, the French government detected fraud related to social benefits equivalent to an estimated EUR 425 million (Comité national de lutte contre la fraude, 2015[18]). In addition, the US Government Accountability Office estimates that improper payments – any payment that should not have been made or was made in an incorrect amount, including underpayments – amounted to nearly USD 141 billion for fiscal year 2017 (US Government Accountability Office, 2019[19]).

While imperfect, such measurements offer baselines for government to assess the effectiveness and efficiency of policies, governance, management and internal controls. Data can also support similar measurements at a micro-level, for instance, within a subset of procurement contracts or among specific beneficiaries of a social benefits programme. These baselines can provide a snapshot for managers to take decisions about controls. In theory, a baseline will allow for monitoring changes in the rates of fraud, corruption or improper payments based on changes in the control environment, which is a critical feedback loop for managerial decision making. For instance, baselines for fraud prevention in social benefit programmes (or other areas) could be established by:

- Examining historical data for fraud to establish a fraud rate, preferably time-series data over a number of years, i.e. what percentage of claims are fraudulent; what percentage of recipients submitted a fraudulent claim.
- Comprehensive large-scale audits or risk assessments can help establish the rate of fraud based on identifying cases of suspected fraud. If fraud is confirmed, results can then be extrapolated to a likely fraud rate based on programme size (e.g. number of recipients; value of detected frauds).
- Random sampling of cases where there is specific focus on finding suspicious cases. Given proper methodological design, identified results can be generalised to entire programmes.

Baselines can also inform performance management systems. For instance, government institutions in Canada (Ontario) and New Zealand have developed fraud reduction-related targets for managers responsible for social benefit programmes. As an example, the following data points could support the development and regular updating of such targets related to social benefit programmes as well as overall performance management over the internal control system:

- the number, percentage and value of fraudulent claims

- the number and percentage of recipients engaging in fraud
- the number and percentage of private providers engaging in fraud
- the number, percentage and value of fraudulent transactions involving different goods and services.

In practice, for many government institutions such activities require skills, capacity and time that is in short supply. Moreover, such approaches to performance measurement provide insights about the effectiveness of controls, but not necessarily their efficiency. Value-for-money is its own measurement challenge, and cost-benefit assessment relies on even richer datasets and information to be carried out.

Looking beyond the walls of their institution, integrity actors can also contribute to government-wide performance evaluation and improvement, using data to substantiate and inform analyses. One way integrity actors do this is by helping policy makers and line ministries to interpret the outputs and outcomes of their own decision making. A range of integrity actors serve this function. For instance, ethics offices and anti-corruption bodies provide feedback on the policies and practices to manage complaints mechanisms, based on their own interpretation of data collected from hotlines, whistleblowing mechanisms and data from asset declarations. Internal audit bodies contribute to decisions about controls and risk treatments based on their audits and risk assessments, which can influence the ability of an organisation to achieve broader objectives. The more the data are of high quality and timely to support this type of work, the more valuable this input can be for real-time decision making.

Implications of ethical use of data, privacy and transparency for integrity actors

A citizen-focused DDPS has the normative frameworks, policies and safeguards in place to ensure the ethical and accountable use of data, protect citizens' privacy and promote transparency (van Ooijen, Ubaldi and Welby, 2019[4]). As discussed, integrity actors rely on a variety of databases and registries to perform their basic duties. These data can include personally identifiable information of citizens. For many applications, anonymised data is insufficient. For instance, forensic auditors, investigators and regulators rely on the ability to use and reuse data with personal information to identify fraudulent patterns and assess criminal behaviour of specific individuals. Nonetheless, to preserve citizen's trust in government institutions, integrity actors can do their part to ensure that their activities strike a balance between oversight, privacy and transparency. Unique identifiers, for example, can be useful for anonymising early stages of analysis, before there is a need to know more about individual cases then simply patterns of behaviour. In addition, integrity actors are well-positioned to lend expertise and insights to the government-wide dialogue about the ethical use of data, privacy and transparency. This section unpacks these issues further.

Integrity actors leading by example to use data ethically and protect privacy

In general, the work of integrity bodies, whether ethics offices, anti-corruption bodies, audit institutions or others, is meant to promote trust in government by ensuring effective and efficient governance. Accountability, transparency and integrity are key principles that underpin their mandates. Integrity actors can further promote these principles by taking practical steps to ensure that ethics, privacy and transparency are considered in their use of data. Failing to consider these issues in their strategy and operations could undermine citizens' trust and integrity actors' own arguments for data access and reuse.

A major challenge for governments is to create the necessary institutional conditions to realise the potential of a DDPS (van Ooijen, Ubaldi and Welby, 2019[4]). Institutional conditions can mean many things, including the various elements of data governance described above, as well as the factors that reflect the unique policy, personnel and technical environment of integrity actors. Some entities have institutionalised the policies around data privacy by dedicating responsible individuals. For instance, the French High

Authority for Transparency in Public Life (Haute autorité pour la transparence de la vie publique), which works to prevent conflicts of interest and manages asset disclosures of public officials, took the concrete step of assigning a "data protection delegate." This individual is in charge of dealing with "any issues susceptible of having an impact in terms of data protection and privacy". According to the law, this delegate "should have the necessary resources at their disposal to accomplish this mission and request any training that they deem useful to maintain their knowledge of the subject" (Haute autorité pour la transparence de la vie publique, 2018[20]).

Organisational codes of conduct are another institutional mechanism that integrity actors can use to promote ethical handling of personal data. In general, ethics laws or codes of conduct serve as the backbone to ensuring integrity in the public service. They act as reference point for public servants regulating ethical norms and principles and conflict of interest (OECD, 2019[21]). In addition to national level codes of conduct, organisational codes of conduct can be targeted at individual contexts and issues. For instance, in Argentina, several entities and state-owned enterprises have adopted their own codes of ethics, tailored to their specific functions and risk profiles (OECD, 2019[21]). Addressing the ethical use of data in institutional codes of conduct can serve as a mechanism to communicate expectations and priorities in the context of the organisation's day-to-day activities. This would help to make the issue of the "ethical use of data" relatable and actionable for employees. Institutional codes of conduct also can be a vehicle for creating consensus, ownership and guidance related to key risk areas across the data value cycle.

In each stage of the data value cycle, from data collection to sharing and reuse, there is a potential for integrity actors to lead by example with regards to the ethical use of data and protecting data privacy. Safeguards can begin early in the cycle, at data collection and access. The United Kingdom's Information Commissioner's Office, an executive non-departmental public body for information rights, offers insights in its 2011 Data Sharing Code of Practice (to be revised in 2019). The code provides frameworks, considerations and good practices for sharing data. It highlights the importance of understanding objectives first, and considering the benefits and risks to individuals or society for sharing data. It also emphasises the need to determine in advance the specific data to be shared, security and controls for use, anonymisation and defining who has access to data (UK Information Commissioner's Office, 2011[22]).

Integrity actors can benefit from taking this systematic approach to data sharing. Data-driven activities to prevent and detect fraud can focus on identification of known suspected criminals or "bad actors," such as the matching of national databases with debarment, sanctions or terrorist watch lists. These techniques are meant to identify whether nefarious entities have infiltrated government services. In general, the public would expect governments to use data for this purpose, given the implications for national and personal security, as well as the integrity of government. Individuals do not have the ability to provide consent for use of these data, as one might consent to use of Internet browsing or health data. However, many data analytics techniques, both manual and automated, cast a wider net in order to identify anomalies and patterns of unknown individuals. For instance, the matching and mining of health or welfare data for fraudulent patterns will take into account entire segments of the population. These techniques can go beyond identifying broad risk areas, such as the identification of risky types of contracts (e.g. single-bid contracts) or individuals (e.g. males under the age of 30), and target specific individuals. Indeed, data of well-meaning citizens can act as a baseline for outliers that could represent fraud or corruption, and therefore innocent citizens by default are a central part of the analysis.

For this reason, it is critical for integrity actors to take steps to maintain citizen's trust by following data-informed codes of conduct, and ensuring proportionality between the value generated from using data and the risks to citizens' privacy. Anonymising data and use of unique identifiers, or creating classification systems and informing citizens, can help to strike a balance and reduce the risks of and concerns over privacy violations. For instance, in Argentina, the OECD suggested a three-tiered classification, ranging from "confidential information" (only accessible by a judicial authority or the Public Prosecutor's Office in a legal case) to "information accessible by the Anti-Corruption Office and the Supreme Court and Magistrates Council of the Nation" and "public information" (OECD, 2019[21]). Transparency about use of data can also

be a useful tool. In the United Kingdom, the British National Fraud Initiative makes use of "privacy notice" that informs citizens about use of their data, as described in Box B.5.

Box B.5. British National Fraud Initiative and the Code of Data Matching Practice

The Audit Commission's National Fraud Initiative was launched in 1996 as the United Kingdom's largest data-matching exercise in relation to fraud. The Serious Crime Act of 2007 enabled bodies, other than those with a mandatory requirement to provide data for the National Fraud Initiative, to volunteer to participate by providing data to the commission (OECD, 2017[24]).

The National Fraud Initiative has enabled participating organisations to prevent and detect more than GBP 300 million fraud and error in the period from April 2016 to March 2018. Approximately 1 200 public and private sector organisations participate in the initiative, among which the public audit agencies in Scotland, Wales and Northern Ireland: each national audit agency carries out data-matching under its own powers, but uses the National Fraud Initiative's systems, processes and expertise.

To increase transparency around this massive data-matching exercise, the National Fraud Initiative has set out a Code of Data Matching Practice that is followed by all organisations that participate in the Cabinet Office's data-matching exercises. The code "creates a balance between the important public policy objective of preventing and detecting fraud, and the need to pay due regard to the rights of those whose data are matched for this purpose." To achieve this goal, the code was informed by the consultation of a range of stakeholders, with the Information Commissioner's office providing input on data protection.

The code notably requires each institution to publish a privacy notice that informs citizens about the specific datasets used, the way they are collected, the purpose of this data-matching exercise and its legal basis, the institutions with which the data are shared, the retention period for the data, and the rights of citizens including complaints mechanisms.

This example illustrates both the necessity of transparency for integrity actors when implementing anti-fraud programmes and the value of their input to inform the creation of codes of practice that safeguard citizen's rights.

Source: GOV.UK (2018[25]), National Fraud Initiative, https://www.gov.uk/government/collections/national-fraud-initiative.

Supporting frameworks for the ethical use of data

Integrity actors are well-positioned to inform government-wide policies and dialogue on the ethical use of data and transparency. For example, there are well-known examples of integrity actors, particularly anti-corruption bodies, playing a critical role in promoting transparency in government and advancing the open data agenda. Open data can help prevent fraud and corruption because it gives the public the opportunity to better monitor the flow and use of public money, thereby shedding light on government activities, decisions and expenditures (OECD, 2017[23]). The effectiveness of open data platforms depends on many of the data governance issues discussed, as well as inter-departmental co-ordination. Integrity actors can take the next step to help the public interpret open data by providing analysis and indicators, as illustrated by the example in Colombia in Box B.6.

Box B.6. The Colombian Observatory of Transparency and Anti-Corruption

The Transparency Secretariat of Colombia created a web portal displaying indicators related to: disciplinary, penal and fiscal sanctions; the Open Government Index (Índice de Gobierno Abierto); and the Fiscal Performance Index (Índice de Desempeño Fiscal). These data sources and indicators are co-ordinated and derived from different sources, including the Prosecutor General's Office (Fiscalía General de la Nación), the Attorney General's Office (Procuradoría General de la Nación), the supreme audit institution (Auditoría General de la República) and the National Planning Department (Departamento Nacional de Planeación). Additionally, the observatory's website provides indicators related to transparency and the implementation status of the public anti-corruption policy elaborated by the Transparency Secretariat.

The indicators related to transparency include: a composite index of accountability; a composite index of the quality of the corruption risk maps; an indicator related to the demand and supply of public information; and a composite index on the regional anti-corruption commissions. The indicators of the public anti-corruption policy are composite indexes (based on overall 24 sub-indexes reflecting the objectives of the Colombian policy) showing the progress made related to five strategic priorities: 1) improving the access to and quality of the public information; 2) making the public management tools for preventing corruption more efficient; 3) enhancing social control to prevent corruption; 4) promoting a culture of legality in the state and society; and 5) reducing the impunity related to corrupt practices. All indicators are also available in excel format (open data), which makes the data readily usable for research, comparisons and media reports. Details on the methodology for elaborating the indicators are also provided.

Source: OECD (2019[24]), OECD Integrity Review of Argentina: Achieving Systemic and Sustained Change, https://doi.org/10.1787/g2g98ec3-en.

As the OECD's working paper on a DDPS explores, integrity actors can play a useful role in supporting the development of normative frameworks that enable a DDPS (van Ooijen, Ubaldi and Welby, 2019[4]). The technical nature of data protection measures has led many countries to create specific bodies to develop such frameworks. For instance, Ireland created the Irish Data Protection Commission and the European Union established the European Data Protection Supervisor, which monitors and ensures the protection of personal data and privacy of individuals. While this is beyond their primary remit, the expertise of integrity actors on ethical issues allows them to identify critical information and to determine priorities in the development of data protection policies and guidelines. Integrity actors can use risk-based approaches to determine which positions are particularly sensitive to integrity risks in order to evaluate the appropriate level of disclosure for different types of public officials depending on the risk-benefit balance (OECD, 2017[24]).

Additionally, the expertise of specific integrity actors, such as ethics offices, can provide useful guidance for institutions that are responsible for developing, implementing and monitoring digital government strategies. Following the example of Hong Kong, China, where the Information Accountability Foundation developed a Model Ethical Data Impact Assessment for the Office of the Privacy Commissioner for Personal Data, integrity actors can support the analysis of how the activities of a DDPS affects citizens (see Box B.8). The Model Ethical Data Impact Assessment looks at the full range of rights and interests of all parties in a data-processing activity to understand how data analytics may impact people in a significant manner, or when data-enabled decisions are being taken without the intervention of people. This type of impact assessment could help public institutions by looking at the rights and interests affected by the data collection, use and disclosure in data-driven activities.

Box B.7. Impact assessments for citizen-centred data processing in Hong Kong, China

In Hong Kong, China, the Office of the Privacy Commissioner for Personal Data commissioned the Information Accountability Foundation, a think-tank specialised in accountability-based information governance, to conduct a consultancy study with the aim of exploring the core values to guide advanced data-processing activities that are ethical and fair to all stakeholders. Published in 2018, the Ethical Accountability Framework for Hong Kong, China provides an analysis and a model assessment framework concerning the legitimacy of data processing.

One element of this framework is the Model Ethical Data Impact Assessment, a step-by-step guidance tool for organisations to identify the full range of rights and interests of all parties in a data-processing activity where advanced data analytics may impact people in a significant manner or when data-enabled decisions are being taken without the intervention of people. The Model Ethical Data Impact Assessment helps organisations identify the goals of specific data-driven activities, their legal implications, their potential benefits and risks, the level of accountability of decision makers and also covers issues of data accuracy and sensitiveness.

While this impact assessment tool was developed with business partners, it could also help public institutions by looking at the rights and interests impacted by the data collection, use and disclosure in data-driven activities. Integrity actors with expertise in ethics could take part in the creation of similar tools and tailor them to the needs of public institutions to help them find a trade-off between the benefits and the risks implied by the use of data.

Source: Information Accountability Foundation (2018[27]), Ethical Accountability Framework for Hong Kong, China, https://www.pcpd.org.hk/misc/files/Ethical_Accountability_Framework.pdf.

Conclusion

Integrity actors are both beneficiaries and contributors to a DDPS. Many integrity actors have government-wide mandates and they occupy a unique position that gives them visibility into the challenges and solutions across government entities for using data to create public value. In addition, they are often grappling with some of the most pressing issues related to data privacy, security and maintaining trust of citizens with regards to the government's use of data. As such, integrity actors can be key collaborators for the CoG and the central entities responsible for advancing a DDPS and digital government strategies. As discussed above, elements of the DDPS framework are beyond the remit of integrity actors, or have limited application to their work. Nonetheless, the key components of a DDPS provides a solid foundation for integrity actors to consider both the whole-of-government and institutional factors that facilitate and inhibit their use of data, so that ultimately they are more effective in taking data-driven, or at a minimum, data-informed approaches to prevent and detect fraud and corruption.

References

ACFE (2018), *Global Study on Occupational Fraud and Abuse: Government Edition*, Association of Certified Fraud Examiners, https://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2018/RTTN-Government-Edition.pdf. [9]

ACFE (2018), *Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse*, Association of Certified Fraud Examiners, https://www.acfe.com/report-to-the-nations/2018. [8]

Comité national de lutte contre la fraude (2015), *Dossier de presse*, Comité national de lutte contre la fraude, Paris, https://www.economie.gouv.fr/files/files/directions_services/dnlf/DOSSIER_DE_PRESSE_Comite_National_de_Lutte_contre_la_Fraude-_Mardi_23_juin_2015%281%29.pdf. [18]

Crime and Corruption Commission (2019), *Corruption Allegations Data Dashboard*, Crime and Corruption Commission, http://www.ccc.qld.gov.au/corruption-prevention/corruption-allegations-data-dashboard/corruption-allegations-data-dashboard-about. [17]

Davenport, T., J. Harris and R. Morison (2010), *Analytics at Work: Smarter Decisions, Better Results*, Harvard Business School Publishing Corporation. [10]

Dilla, W. and R. Raschke (2015), "Data visualization for fraud detection: Practice implications and a call for future research", *International Journal of Accounting Information Systems*, Vol. 16, pp. 1-22, https://doi.org/10.1016/j.accinf.2015.01.001. [6]

European Commission (20014), *Guidance for the Commission and Member States on a Common Methodology for the Assessment of Management and Control Systems in the Member States*, https://ec.europa.eu/regional_policy/en/information/publications/guidelines/2014/guidance-forthe-commission-and-member-states-on-a-common-methodology-for-the-assessment-ofmanagement-and-control-systems-in-the-member-states. [28]

European Commission (2018), *Interoperability of Security and Border Management Systems with Customs Systems: Assessment Report of the Practitioners*, European Commission, Brussels, http://www.statewatch.org/news/2019/mar/eu-council-interoperability-customs-5574-19.pdf. [3]

European Commission (2015), *Fraud and Error in the Field of EU Social Security Coordination*, Publications Office of the European Union, https://ec.europa.eu/social/BlobServlet?docId=18644&langId=en. [15]

European Court of Auditors (2019), *Tackling fraud in EU Cohesion Spending: Managing Authorities Need to Strengthen Detection, Response and Coordination*, https://op.europa.eu/webpub/eca/special-reports/fraud-in-cohesion-6-2019/en/#chapter3. [29]

Gatto, M. (2015), *Making Research Useful: Current Challenges and Good Practices in Data Visualisation*, University of Oxford and the Reuters Institute for the Study of Journalism, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/research/files/Making%2520Research%2520Useful%2520-%2520Current%2520Challenges%2520and%2520Good%2520Practices%2520in%2520Data%2520Visualisation.pdf. [16]

GOV.UK (2018), *National Fraud Initiative*, https://www.gov.uk/government/collections/national-fraud-initiative. [25]

Haute autorité pour la transparence de la vie publique (2018), *Règlement intérieur*, Haute autorité pour la transparence de la vie publique, Paris, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000036970810&dateTexte=&categorieLien=id (accessed on 19 July 2019). [20]

Information Accountability Foundation (2018), *Ethical Accountability Framework for Hong Kong, China*, Information Accountability Foundation, https://www.pcpd.org.hk/misc/files/Ethical_Accountability_Framework.pdf. [26]

OAG-WA (2016), *Audit of Payroll and Other Expenditure Using Data Analytic Procedures*, Office of the Auditor General Western Australia, https://audit.wa.gov.au/wp-content/uploads/2016/05/report2016_06-DataAnalytics.pdf. [12]

OECD (2019), *Analytics for Integrity: Data-Driven Approaches for Enhancing Corruption and Fraud Risk Assessments*, OECD, Paris, http://www.oecd.org/gov/ethics/analytics-for-integrity.pdf. [5]

OECD (2019), *Digital Government Review of Argentina: Accelerating the Digitalisation of the Public Sector*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/354732cc-en. [2]

OECD (2019), *OECD Integrity Review of Argentina: Achieving Systemic and Sustained Change*, OECD Publishing, Paris, https://doi.org/10.1787/g2g98ec3-en (accessed on 1 July 2019). [21]

OECD (2019), *Survey of the OECD Auditors Alliance*, OECD, Paris. [7]

OECD (2017), *Algorithms and Collusion: Competetion Policy in a Digital Age*, OECD, Paris, http://www.oecd.org/daf/competition/Algorithms-and-colllusion-competition-policy-in-the-digital-age.pdf. [1]

OECD (2017), *Compendium of Good Practices on the Use of Open Data for Anti-corruption: Towards Data-driven Public Sector Integrity and Civic Auditing*, OECD, Paris, http://www.oecd.org/corruption/g20-oecd-compendium-open-data-anti-corruption.htm. [23]

OECD (2017), *Internal Control and Risk Management for Public Integrity in the Middle East and North Africa*, OECD, Paris, https://www.oecd.org/gov/ethics/corruption-risks-internal-control-mena.pdf. [27]

OECD (2017), *OECD Integrity Review of Mexico: Taking a Stronger Stance Against Corruption*, OECD Public Governance Reviews, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264273207-en. [24]

OECD (forthcoming), *Public Integrity Handbook: Chapter 3 on Strategy*. [11]

TCU (2016), "Geotechnologies and monitoring of Sustainable Development Goals by supreme audit institutions", *Revisita do TCU*, Vol. 137, https://revista.tcu.gov.br/ojs/index.php/RTCU/issue/view/68/102. [14]

TCU (2016), "InfoSAS: A data mining system for production control of SUS", *Revisita do TCU*, Vol. 137, https://revista.tcu.gov.br/ojs/index.php/RTCU/issue/view/68/102. [13]

UK Information Commissioner's Office (2011), *Data Sharing Code of Practice*, UK Information Commissioner's Office, London, https://www.pdpjournals.com/docs/88438.pdf. [22]

US Government Accountability Office (2019), *Improper Payments: Selected Agencies Need Improvements in their Assessments to Better Determine and Document Risk Susceptibility*, US Government Accountability Office, Washington, DC, https://www.gao.gov/assets/700/696384.pdf. [19]

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]

Annex C. Data-driven human resources management: Enabling the strategic use of human resources data for a high-performing civil service

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

Introduction

At the age of the digital transformation, governments have understood the growing importance of the value of data as a foundation for improved policy making, service delivery and ongoing performance management. In this context, many OECD countries are aiming to develop a data-driven public sector (DDPS), one which recognises data as an asset, integral to policy making, service delivery, organisational management and innovation. The strategic approach for DDPS can have a positive impact on the results governments deliver through evidence-based policy making and data-informed service design (van Ooijen, Ubaldi and Welby, 2019).

In the same manner, data-driven human resources management (DDHRM) pursues strategic human resources (HR) management by using HR data. In the past, HR policy had a tendency to rely on past practices or a decision maker's experience or intuition, with no scientific or objective evidence. Today, workforce data from multiple sources present opportunities to manage public employees through evidence-based HR policies. Governments are thus increasingly able to recruit, deploy, train, motivate and retain their employees in a scientific and analytic way based on objective HR data.

The 2019 OECD Recommendation of the Council on Public Service Leadership and Capability presents 14 principles of a fit-for-purpose public service. It includes a recommendation to develop "a long-term, strategic and systematic approach to people management … using HR and workforce data for strategic and predictive analytics, while taking all necessary steps to ensure data privacy" (OECD, 2019).

Public services are collecting more data on their public employees today than ever before. Demographic data provide a snapshot of the workforce and enable a better understanding of skill sets, workforce diversity and age. Administrative data show employment trends and patterns that can indicate organisational health through, for example, job attractiveness, the efficiency of HR processes and mobility/turnover rates. Data from employee surveys can provide rich indications of employees' engagement and satisfaction with their work and working environment.

HR data are abundant. Today, in the era of "big data", the amount of data available to inform strategic workforce management has exploded and thanks to the development of information technology, it can be processed and utilised more efficiently. These data can be collected from both internal (e.g. human resources information systems or employee surveys) and external (e.g. social media or labour market trends) sources. However, most countries only collect HR data, as they struggle with scientifically analysing, insightfully interpreting and proactively using them for better management decision making and HRM policy development and delivery. They are still not sure how to make sense of all these data or what to do with them; there are a lot of challenges in making DDHRM work well. Data scientist is not yet a common job profile within HR departments.

This case study will focus on how a DDHRM can be applied to strategic human resources management in order to attain organisational goals effectively and subsequently identify challenges governments may face in establishing a DDHRM.

Overview

Definition

DDHRM is also referred to as evidence-based HRM, HR analytics and workforce analytics in the literature. Evidence-based HRM is a decision-making process combining critical thinking with use of the best available scientific evidence and business information. It is composed of four elements: 1) the best available research evidence; 2) organisational facts; 3) metrics and assessments; 4) practitioner reflection and judgement and the consideration of the affected stakeholders (Rousseau and Barends, 2011). HR analytics is an HR practice enabled by information technology that uses descriptive, visual and statistical

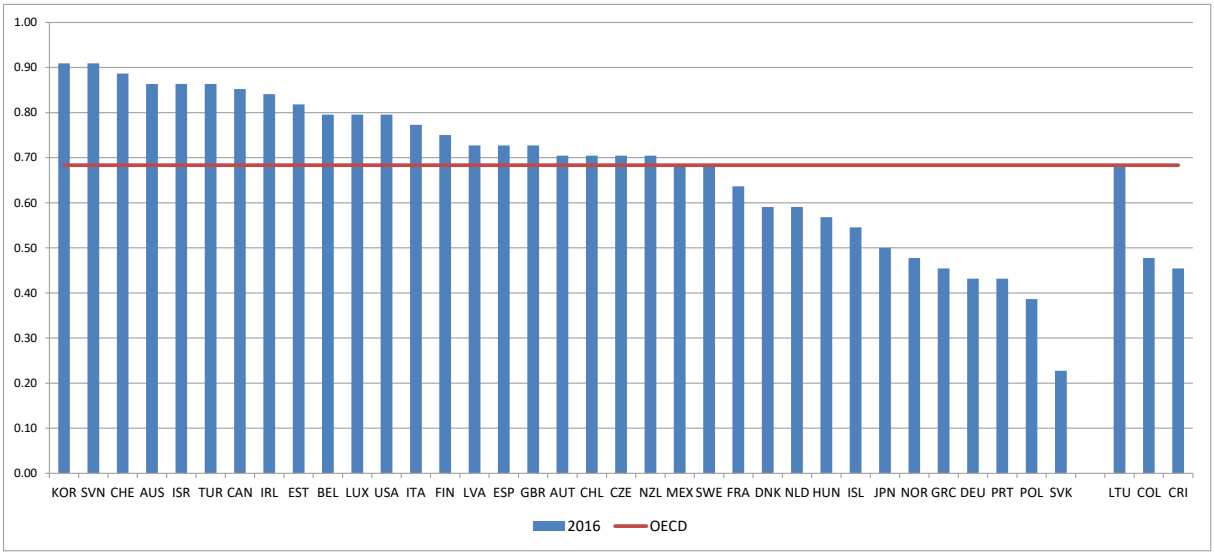
analyses of data related to HR processes, human capital, organisational performance and external economic benchmarks to establish business impact and enable data-driven decision making (Marler and Boudreau, 2017). HR analytics is the systematic identification and quantification of the people drivers of business outcomes (Heuvel and Bondarouk, 2016). This definition encapsulates HR, people, talent and human capital analytics that focus on the individual. Workforce analytics is people analytics on a larger scale. It is about scaling up the data from multiple individuals to assess trends on the broader workforce level. Sometimes it is more narrowly used to discuss workforce planning.

In this case study, DDHRM is defined as a strategic process aiming for better HR decisions and policies throughout the government by collecting, measuring and using HR data such as demographic data, administrative data (including pay data and turnover), employee perception data (employee surveys) and performance data. DDHRM is based on data and evidence instead of intuition or personal experience.

Collection and use of human resources data in OECD countries

The OECD has collected and used quantitative and qualitative HR data for comparative analysis across OECD countries in the field of public sector human resources management and civil service reform strategies. The 2016 Survey on Strategic Human Resources Management in Central Governments of OECD Countries gathered data related to the broad trends of public employment and HRM across OECD countries and provided OECD countries with a better picture of where they stand compared to other countries in these fields. This included a new set of questions on the collection and use of data for HRM. The survey looked at three types of data: administrative data, employee survey data and employee performance data. In Government at a Glance 2017, the OECD presented the results of a survey which looks at the amount and type of administrative HR data collected by OECD countries, which shows a wide variation (OECD, 2017).

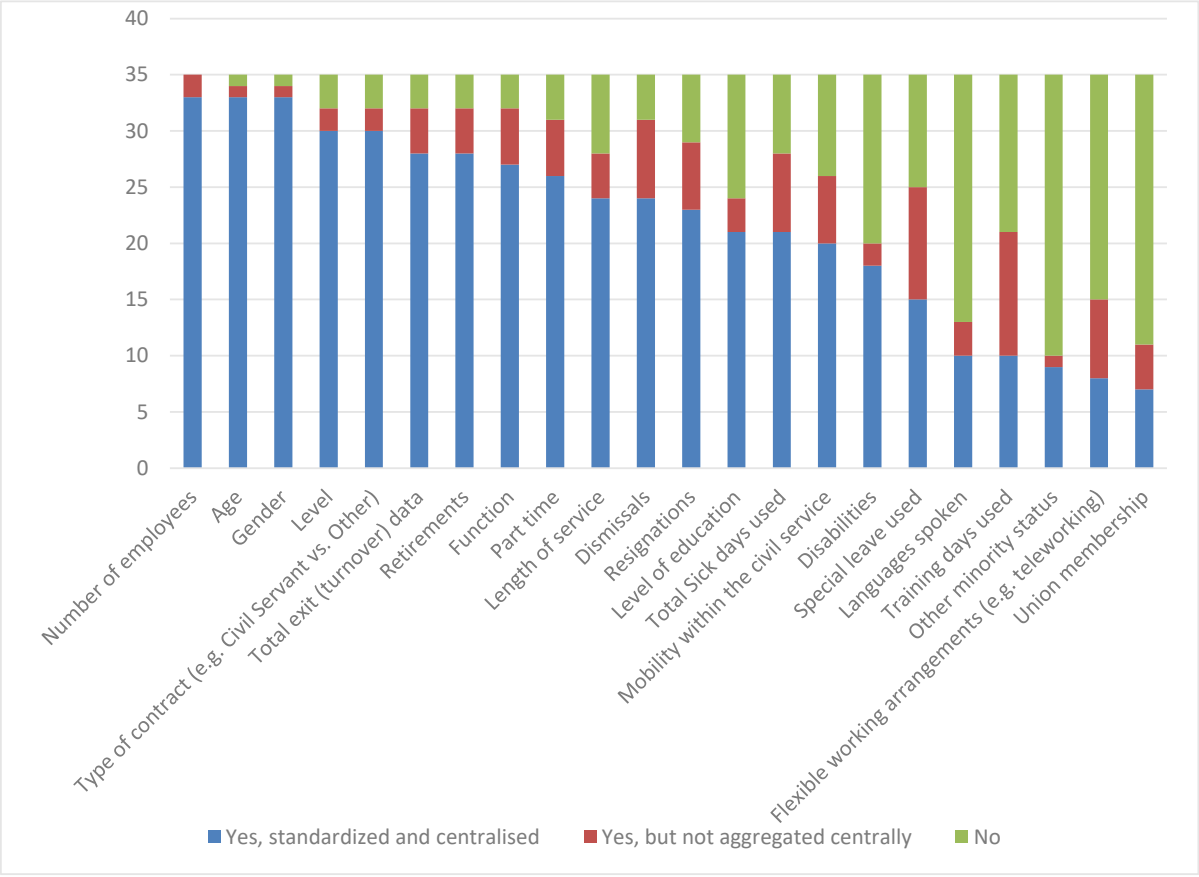
Figure C.1. Collection and availability of administrative human resources data



Source: OECD (2017), Government at a Glance 2017, https://doi.org/10.1787/gov_glance-2017-en.

The results of the survey show that most OECD countries collect and centralise basic HR data, such as number of employees, age and gender. However, relatively fewer countries gather deeper and more meaningful HR data related to working conditions or organisational culture, such as minority status, flexible working arrangements and union membership. Data related to training, leave and mobility are often not aggregated centrally, when they are collected by ministries.

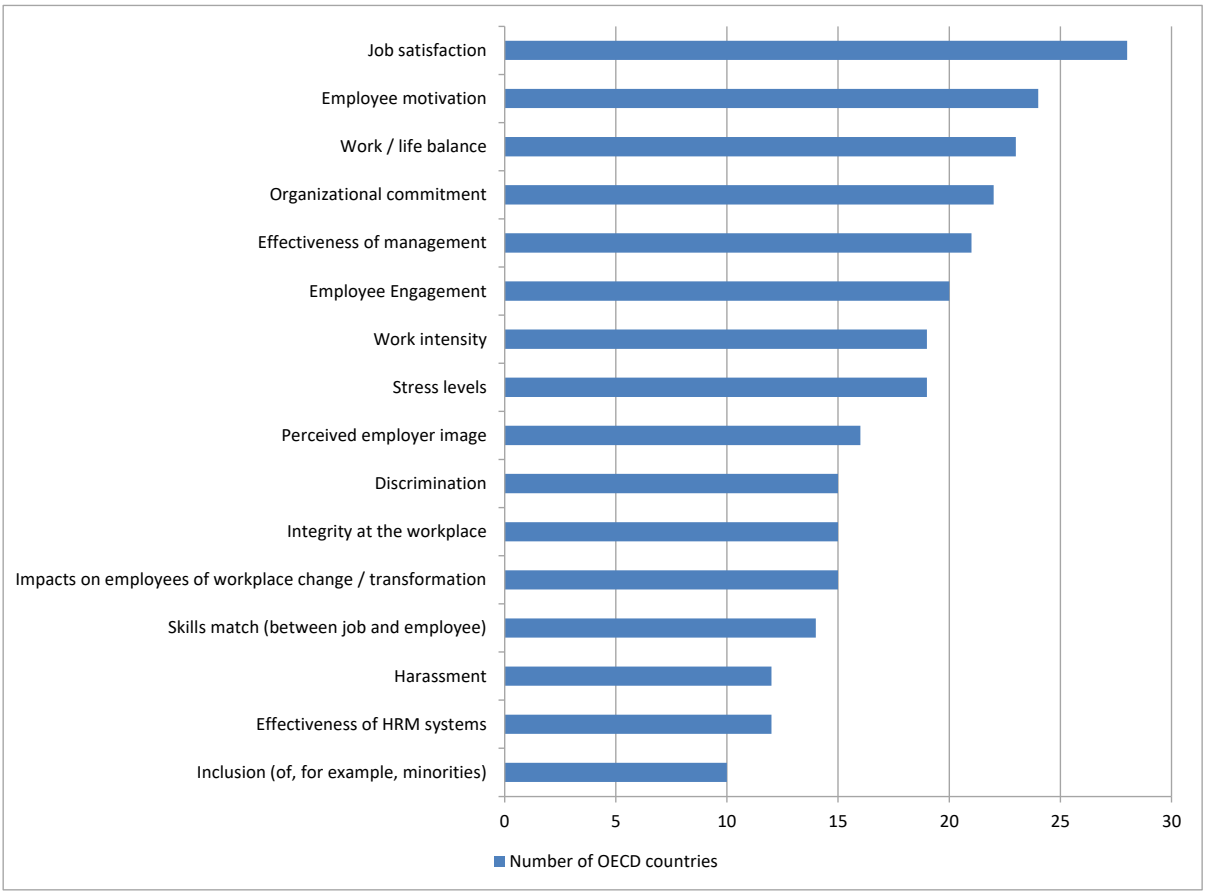
Figure C.2. Human resources data collected by OECD countries, number of countries, 2016



Source: 2016 OECD Survey on Strategic HR Management in Central/Federal Governments.

Employee surveys are another important source of HR data, and most OECD countries use them, to differing degrees. Centralised civil service-wide surveys are often run at regular intervals, and complemented by specific surveys carried out by individual agencies and ministries. OECD countries measure employee perceptions of job satisfaction, employee motivation and work/life balance through employee surveys. On the other hand, relatively fewer countries use these tools to measure inclusion, harassment and effectiveness of HRM systems.

Figure C.3. Aspects assessed in employee surveys in central/federal governments, 2016



Source: 2016 OECD Survey on Strategic HR Management in Central/Federal Governments.

Box C.1. Benchmarking employee engagement in OECD countries

The OECD has been tracking and analysing the use of employee surveys in central governments since its 2016 report on Engaging Public Employees for a High-Performing Civil Service (OECD, 2016). The report looked at the promising use of such surveys to develop data-driven people management by comparing indicators such as employee engagement across ministries and agencies. Indeed, data on engagement could be analysed by team, organisation/sector, demographic group, profession, as well as over time, to identify drivers and outcomes of employment and inform the design of human resources management policies to improve employee motivation.

Although many civil services were measuring engagement in their employee surveys, each was following their own definition of engagement, along with differing survey questions, which did not permit comparison. Therefore, in 2016, the OECD created an informal working group to develop a standard questionnaire module on employee engagement. The objectives of this exercise were three-fold:

1. to permit international comparison across countries (and common sectors, such as education, health, etc.) on employee engagement to identify trends and good practices
2. to exploit an international database to explore the key drivers of engagement and its impacts on key outcomes such as team and organisational performance, and citizen satisfaction with public services

3. to incorporate results from the standard module as outcomes data on public employment policy into the Government at a Glance database, the leading source of comparative international key performance indicators on public management for OECD member and partner countries.

Following a literature review and testing exercise, the working group has settled on the following analytical framework for measuring engagement: employees' work engagement and job satisfaction; organisational commitment; and public service commitment and motivation.

Figure C.4. OECD analytical framework for benchmarking employee engagement

The following survey questions were selected for each dimension from existing modules in the academic literature (such as the Utretcht Scale), as well as other countries' surveys.

Job satisfaction

Overall, I am satisfied with my job.

Work engagement

My job inspires me.

The work I do gives me a sense of accomplishment.

Organisational engagement

I feel a strong personal attachment to my organisation.

I identify with the mission of my organisation.

Public service motivation

It is important to me that my work contributes to the common good.

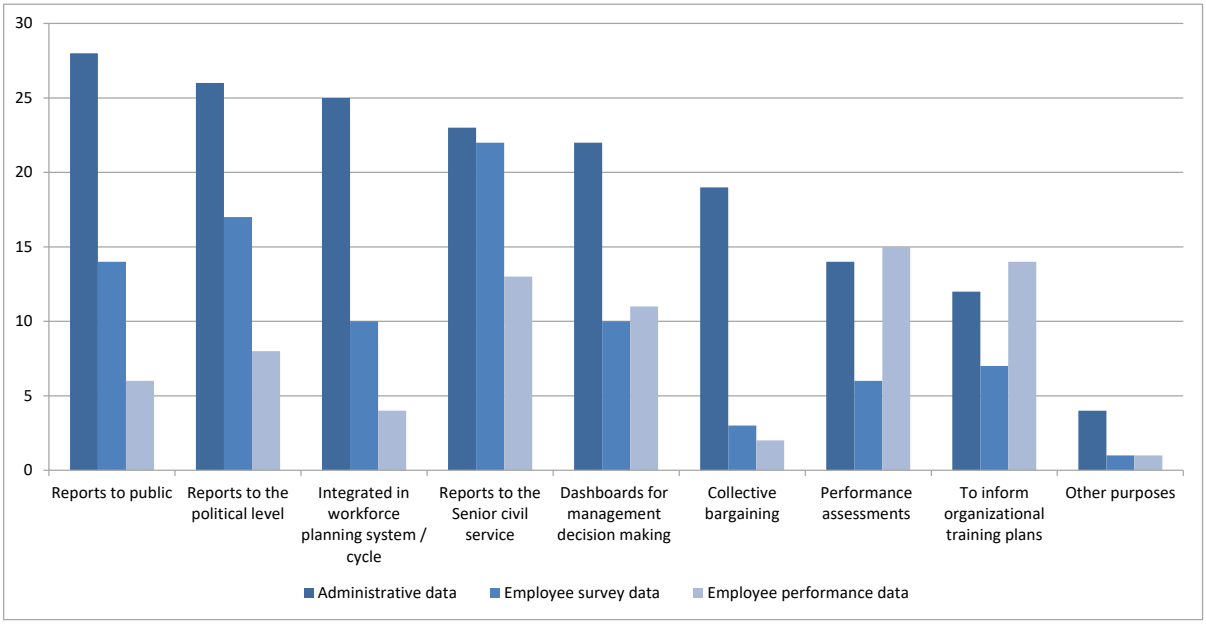
Responses will be collected through a 1-5 Likert Scale, with data reporting to the OECD.

Preliminary results from participating countries are expected by the end of 2021. For further information on how to participate in the working group or the benchmarking exercise, please contact PEM@oecd.org.

When it comes to employee performance data, less than half of the OECD countries report collecting these data centrally. This may be due to the difficulty of objectively measuring employee performance in ways that are comparable across diverse job types and working conditions.

In most OECD countries, administrative data are used for reporting to the public and employee survey data are used for reporting to the senior civil service. Employee performance data are mainly used for assessing performance or informing organisational training plans.

Figure C.5. Use of human resources data in central/federal governments of OECD countries, number of countries



Source: 2016 OECD Survey on Strategic HR Management in Central/Federal Governments

Opportunities and application

The OECD framework for understanding the opportunities of a DDPS (Figure C.6) identifies three areas in which data-driven initiatives are being developed to support the decision making process across policy areas and levels of government: 1) anticipatory governance; 2) design and delivery; and 3) performance management (van Ooijen, Ubaldi and Welby, 2019).

Figure C.6. Opportunities for a data-driven public sector

Anticipatory governance

- Forecasting to proactively identify developments and future needs
- Foresight to prepare for multiple plausible alternative outcomes

Design and delivery

- Better predicting policy solutions
- Engaging with citizens as co-value creators
- Responding better to citizens' needs

Performance management

- More efficient use of resources
- Increase in resources
- Higher quality and evaluation
- Continuous improvement

Source: van Ooijen, C., B. Ubaldi and B. Welby (2019[1]), "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.

In this case study, the framework of DDHRM will adjust the OECD framework of DDPS to suit HR functions. DDHRM creates the opportunities in two main areas: 1) forecasting and planning; and 2) monitoring and evaluation.

(Future) forecasting and planning

Based on past and present data from various sources, predictive analytics involves the development of statistical models and forecasts to help identify future workforce and talent pool trends. Anticipating such trends gives managers and organisations a critical head start in preventing, mitigating or encouraging developments, ultimately saving them costs and helping improve performance.

The possibilities for predictive HR analytics are still being explored; however, a few common applications have thus far included strategic workforce planning, improving diversity and inclusion, and retaining top talent.

1. Strategic workforce planning

Strategic HRM aligns people management with the strategic goals of public sector organisations (OECD, 2011). Strategic workforce planning for strategic HRM is crucial to predict workforce change according to change in the administrative environment – such as demographic, technology and economic situations – and prepare for recruiting needed talents. Strategic workforce planning is a core HRM process that helps to identify, develop and sustain the necessary workforce skills. In doing so, it also contributes to the career and lifestyle goals of employees and ensures the continued effective performance of organisations. Workforce planning is a dynamic process that ensures that the organisation has the right number of people with the right skills in the right place at the right time to deliver short and long-term organisational objectives. Workforce planning aims to reach an optimal combination of available personnel budget and appropriate number of human resources endowed with the required skills to bring about organisational objectives. Workforce planning not only identifies mission-critical occupations and the essential competencies to meet organisational goals, but also detects competency gaps (Huerta Melchor, 2013).

Box C.2. Data-driven human resources planning in the OECD Recommendation of the Council on Public Service Leadership and Capability

The OECD's Recommendation of the Council on Public Service Leadership and Capability was adopted in 2019, and contains 14 principles for a fit-for-purpose civil service. It specifically recommends that governments "develop public employment systems that foster a responsive and adaptive public service able to address ongoing and emerging challenges and changing circumstances", in part by:

Developing a long-term, strategic and systematic approach to people management based on evidence and inclusive planning that:

1. is informed by evidence-based assessment of skills needed and skills available to meet current and future core business requirements, using human resources and workforce data for strategic and predictive analytics, while taking all necessary steps to ensure data privacy
2. sets strategic direction and priorities with input from relevant stakeholders, in particular public servants and/or their representatives, and the management accountable for implementation
3. considers all relevant aspects of people management and ensures alignment with strategic planning processes of the government, including budget and performance management
4. includes appropriate indicators to monitor progress, evaluates the impact of human resources policies and processes, and informs decision making.

Source: OECD (2019[2]), Recommendation of the Council on Public Service Leadership and Capability, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0445.

DDHRM can help to forecast a list of potential gaps in the workforce by looking at long term trends. For example, various data can be analysed and predicted when analysing the current state and supply of the workforce and forecasting the trend and needs of the future workforce. This can include, for example, workforce movement (workforce inflows such as new hires, promotions and transfers; workforce outflows such as resignations, retirements and involuntary terminations), the differences between the present available workforce level and the workforce level which will be required in the future, and gaps in competencies and numbers of employees in each job area. This information can be used to design a strategic workforce plan to close workforce gaps in each job area and strengthen organisational competitiveness in the future.

One example is the Mexican Ministry of Energy, which is using workforce planning to identify current and future skills gaps in oil and gas occupations over a ten-year horizon. “The model leverages a number of adjustable macroeconomic variables such as oil price and exchange rates that correlate strongly to the demand and supply of skilled labour. Based on an understanding of these gaps in critical skills, the ministry is able to work proactively with multiple stakeholders to address them. Building off from this initiative, the ministry has expanded the use of workforce planning and analytics to cover other sectors it is responsible for, such as renewable energy and sustainability” (Deloitte, 2016).

2. Retaining top talent/targeted retention

While strategic workforce planning may include employee turnover as one input to its modelling, predictive analytics can delve deeper, specifically into voluntary turnover with a view to reducing this type of attrition in organisations, and particularly among top performers. Indeed, employee churn costs employers greatly in terms of lost productivity and institutional knowledge, but also in sunk costs in recruitment and learning and development. Turnover also affects citizens in terms of interrupted policies and in the quality of service delivery. The United Kingdom’s Institute for Government published a report estimating that excessive turnover in departments costs the civil service between GBP 36 million and GBP 74 million each year in recruitment, training and lost productivity (‘Moving On”, 2019). As labour markets become increasingly competitive, predictive analytics is being used to help pre-empt and advert involuntary turnover, and particularly in certain groups of employees.

Such predications, however, must be based on robust models of the drivers of voluntary turnover. Several studies have tried to identify the specific causes of resignations in public services. Based on certain “signals”, this application of predictive analytics relies on models using past/present data to identify employees at “high risk” of attrition.

Several studies have attempted to tease out valid predictors of voluntary turnover. The results have found a multitude of drivers. Indeed, a literature review of existing attempts found that the strongest predictors for voluntary turnover were age, tenure, pay, overall job satisfaction, and employee’s perceptions of fairness. Other similar research findings suggested that personal or demographic variables – specifically age, gender, ethnicity, education and marital status – were important factors in the prediction of voluntary employee turnover. Other characteristics that studies focused on are salary, working conditions, job satisfaction, supervision, advancement, recognition, growth potential and burnout (Punnoose and Pankaj, 2016).

While most studies have focused on private sector employees, public services are beginning to conduct similar studies. In the United States, researchers used a database which included information on federal civil servants from the Office of Personnel and Management, including such dimensions as age, agency type, gender, salary level, geographical location of employee, length of service, occupation type, pay plan and work plans (i.e. temporary, full-time, etc.). The results of logistic regressions revealed a significant reduction in the probability of an employee quitting as his/her service length increases; odds increasing or decreasing depending on employee age; and odds of quitting are lower if the employee is in the standard

pay plan. Comparing age and length of service, we found resignations spike around 6.25 years of service, regardless of age (Frye et al., 2018).

Using such models, HRM professionals and managers can then intervene by offering salary increases, professional opportunities or changing working conditions (i.e. flexible work, telework) suited, depending on the level of granularity of the data, to teams'/individuals' own preferences. However, many note the ethical concerns of predictive analytics for employee attrition arguing that the data can suggest dangerous and unfounded correlations that may lead managers to draw incorrect conclusions. For instance, a relationship between gender and attrition may lead unethical managers to discriminate against certain potential recruits. Additionally, some argue inclusion of certain data will confound results. For instance, self-reported data may not always be accurate, especially if employees believe their responses are being used for predictive modelling.

3. Predicting inclusive leadership in the public service

DDHRM can also help to meet specific future targets to develop the workforce. For example, the Public Service Commission of the state of New South Wales in Australia has adopted a data-driven approach to designing and monitoring progress on diversity and inclusion policies (OECD, 2019).

In order to monitor agencies' expected trajectories in meeting diversity targets, the Public Service Commission has developed a model that predicted – based on current recruitment and separation behaviour across the public sector – what the proportion of women in senior leadership roles would be. This was then extended to each cluster and became the starting point to demonstrate that unless a framework of high-impact whole-of-government initiatives were in place, there would be little movement of the rate. Thanks to this predictive model, the Public Service Commission arrived at the view that to achieve 50% of women in senior roles by 2025, the public sector needed six out of every ten appointments to senior roles to shift from four out of ten. Current data have shown this rate is now at 5.5 out of 10.

These cases illustrate the potential for forecasting and planning for better HR policies through DDHRM. By focusing on a set of future goals, multiple data sources can be combined to develop insights on current challenges that may be impeding the achievement of these goals. In all of the cases listed above, data-driven scenarios can help to see various versions of the future. Another useful point is that workforce data are easily accessible since data sources are internal. Most HR offices have access to key data points around the composition of their workforce, mobility patterns and bottlenecks. The challenge is in making these data useful and investing in the skill sets needed to analyse them and drive towards insights and solutions.

(Present) monitoring and (past) evaluation

Following the DDPS framework, this area shows how HR data can be used to better understand the current state of the workforce and HR service delivery. HR data can be used to address problems by reflecting the needs of various stakeholders, such as HR staff, employees and other interested parties, and improving the effectiveness and efficiency of HR policies by providing feedback to the HR decision-making process through evaluation of the impact of HR policies. When data are collected on an ongoing basis and structured effectively, DDHRM can significantly reduce the amount of time between implementation and evaluation – identifying problems as they arise and enabling policy interventions, almost in real time. These two areas are dealt with together in this case study.

Monitoring HR policies

Given that human resources management is a strategic lever to achieve government objectives, most OECD countries try to innovate their approaches to HRM. The examples that follow show how HR data collected through monitoring and evaluation can be used to spark innovation in the design and delivery of people management policies and processes.

US HRStat Programme

HRStat is a data-driven review process intended to improve human capital outcomes, enhance the performance capacity of agencies in achieving their strategic goals and objectives, and create a supportive culture for the use of data-driven reviews that inform agencies' human capital decision making. The Office of Personnel Management introduced HRStat to the federal human capital community in 2013. (US Office of Personnel Management, 2017)

HRStat reviews focus on specific HR challenges, identified and explored through data analysis, monitoring and evaluation. As such, HRStat reviews do not merely present HR data on topics such as attrition rates, completion of performance evaluation plans, numbers of completed hiring decisions or training participation rates. Rather, federal agencies engage in data-driven reviews of HR areas that are in need of improvement, innovation or improved cost effectiveness.

For example, agencies may use the HRStat reviews to assess work demands, emerging mission imperatives and workforce trends likely to affect skills needs. They can also use them to evaluate HR strategies and interventions designed to reduce or eliminate competency gaps in vital positions, or to understand why certain interventions may help alleviate attrition risk among employees in high-impact positions. In this way, HRStat helps to create empirical evidence to inform HR decision making and provide agencies with a continuous means of learning and gaining insights for improving HR processes. Conducting HRStat reviews also enables agencies to evaluate progress, refine strategies and develop demonstrable quantifiable evidence of successful human capital outcomes.

Table C.1. Common metrics agencies have used in HRStat reviews

Categories	Metrics
Federal Employee Viewpoint Survey	Engagement Index, Workload Index, Inclusion Quotient, Intention to Leave, Talent Management Index, Job Satisfaction Index, Inclusive Work Environment Index, Leadership Index, etc.
Hiring metrics	Time to hire, number of applicants, candidate quality, demographics/diversity, disability status, measuring applicants' satisfaction, etc.
Training	Completion of training, satisfaction with training, mentoring experience satisfaction, etc.
Performance management	Performance appraisal, performance management process analysis
Agency personnel database sources	Promotions, demographics (occupation, years of service, diversity, veterans, disability), telework and alternative work schedule, health and wellness, attrition, etc.

Source: (US Office of Personnel Management, 2017[14])

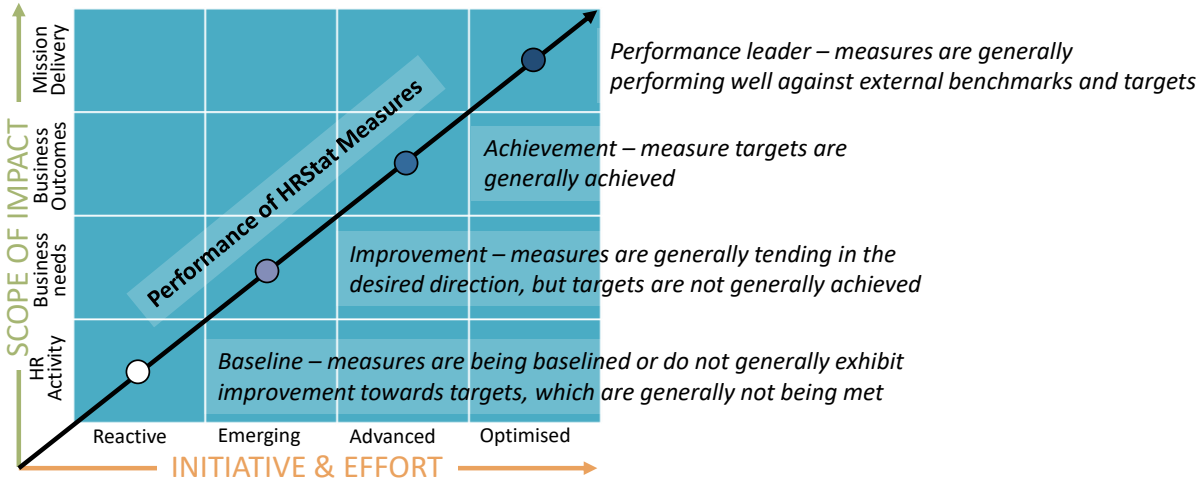
Another aspect of the HRstat programme is the Maturity Model (see Figure C.7), which provides a diagnostic framework to assess the maturity level of an agency's DDHRM. The Maturity Model serves as a practical and aspirational roadmap that will help agencies identify areas for improvement and enable them to monitor their progress over time.

The HRStat Maturity Model is conceptualised in terms of three components:

1. Scope of impact measures the degree to which metrics are integrated into the measurement of agency mission accomplishment.
2. Initiative and effort measures the degree to which an agency has developed the capacity to use HR data to inform decision making across the agency.
3. Performance of HRStat measures the degree to which an agency's metrics are advancing to achieve targeted improvements and are validated against external benchmarks.

For each of these three components, there are four maturity levels (reactive, emerging, advanced, optimised). In describing the four maturity levels, the HRStat Maturity Model designates five domains of consideration: analytics, technology, talent/staff, collaboration, and leadership.

Figure C.7. HRStat Maturity Model



Source: (US Office of Personnel Management, 2017[14])

Korea's HR innovation diagnosis indicators

Korea provides another example of DDHRM for monitoring and evaluation. High demand for integrity and public confidence in the government in Korea requires transparent and accountable personnel management to better respond to public demand. The establishment of the Ministry of Personnel Management (MPM) in charge of HR innovation in 2014 has increased the demand for effective and responsive personnel management for the public. Starting in 2015, HR Innovation Diagnosis Indicators were developed and have been used to carry out objective assessments (Korea Ministry of Personnel Management, 2018).

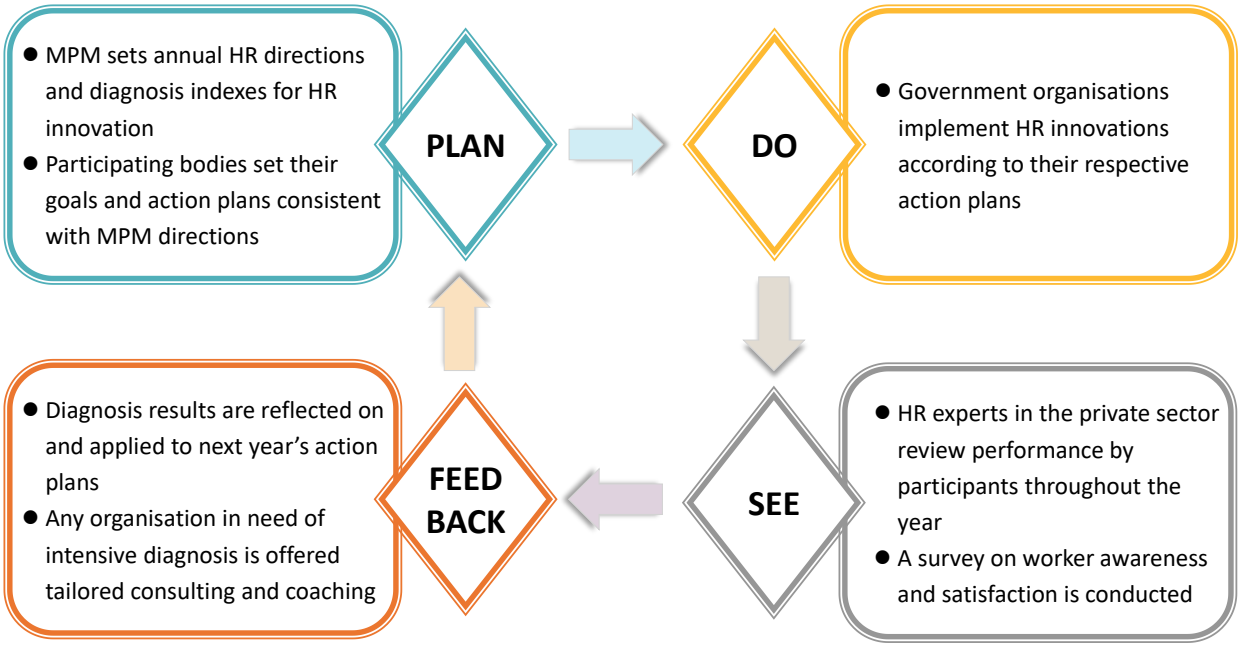
Based on the indicators, the MPM assesses each government organisation's HR innovations and provides feedback to enhance its innovation capability through a cycle of plan, do, see and feedback.

The indicators are composed of five fields:

1. implementation capacity measures agencies' commitment to HR innovations and excellence in HR innovation plans
2. employment measures open and diverse recruitment
3. human resource development measures employees' perceptions and awareness of development opportunities and organisational efforts to develop their workforce

4. expertise and performance management measures compliance and observance of various programmes to ensure professional standards, including performance management
5. improvement of working environment and conditions measures efforts to encourage the use of personal days off and a flexible work system, and attempts to fight discrimination among government workers.

Figure C.8. Measuring process



Source: Korea Ministry of Personnel Management, 2018

In order to measure these indicators, the MPM uses a range of methods. Quantitative methods include indicators such as open positions and employment rates, and increase in employment of female managers. These are complemented by qualitative methods, for example excellence in HR innovation plans and appropriateness of education and training plans; as well as awareness and satisfaction survey methods, such as awareness of flexible working options and satisfaction with development opportunities.

As a part of collaborative innovation, the MPM sets indicators with participating government bodies and external experts after in-depth consideration. Moreover, indicators are adjusted on an annual basis, subject to the MPM's annual innovation directions, feedback from participating bodies and changes in environments.

The MPM provides feedback and incentives (e.g. a long-term overseas training) to participating agencies and offers lagging agencies tailored consulting upon request. Furthermore, the MPM hosts quarterly workshops to spread good practices and set benchmarks.

Challenges to implementing DDHRM in the public sector

- Public administrations face several barriers in implementing DDHRM:
- technical barriers (i.e. related to IT infrastructure and resources)
- legal barriers (i.e. privacy concerns)
- human resources barriers (i.e. lack of skills and knowledge among HRM professionals and senior managers).

These challenges are often why HRM practitioners in public sector organisations are perceived as falling behind their private sector counterparts in embracing DDHRM more whole-heartedly. This section discusses these issues in further detail, with a view to help practitioners anticipate potential obstacles and ensure they have the right foundations in place to successfully adopt DDHRM practices going forward.

IT governance, infrastructure and resources

The power of DDHRM originates from the compilation and analysis of data from across entities and organisations. As described earlier, there are multiple types of valuable data (i.e. pay, tenure, perception data, information on employees' work experiences, education and performance, and HRM metrics like churn, sick leave, etc.) that commonly feed into DDHRM platforms and analysis. The challenge is integrating the data from several individual organisations/databases when each uses different formats or indicators. Ensuring data accuracy and comparability in such cases is difficult unless some prior method of quality control and standardisation is in place. This challenge is compounded even further as data from external (non-governmental) sources, such as from social media, becomes increasingly incorporated into DDHRM exercises.

Moreover, the shift towards DDHRM requires that organisations change the ways in which they collect and store data. This entails not only changes to the IT systems themselves – including the adoption of cloud computing, DDHRM platforms and software, etc. – but also to underlying business processes. For example, maintaining payroll, timekeeping or performance data will need to adapt to the new IT systems and methods of data collection, entry and storage. Such reforms entail not only changes to processes, but also require financial resources to develop and install DDHRM tools and train staff to transition to new systems. However, fairly recent austerity measures in the public sector have limited IT spending, and many managers still remain unconvinced of the business case in favour of such investments.

In response to these challenges, most organisations have adopted a piecemeal approach to compiling relevant data, starting with what is available and slowly building more comprehensive databases in partnership with other organisations (finance, payroll, human resources, etc.). Building consensus, excellent communication and support (in the form of written guidance, personnel or IT resources) is often necessary in bringing other organisations on board. Furthermore, monetising the advantages of adopting DDHRM tools and techniques, in terms of improved performance and organisational outcomes, as well as sharing good practices and experiences from early adopters in the public administration, have proven to help improve buy-in and participation from managers.

Legal constraints, privacy and confidentiality

A second major barrier to adopting DDHRM in the public sector are legal constraints around the types of information that government organisations can collect, store and analyse. Indeed, information collected and maintained on employees is sensitive – from their pay to performance and health or other personal information. In many OECD countries, there are strict regulations that protect employee privacy. The EU's General Data Protection Regulation, for example, defines high-risk data as those which are "likely to result in a high risk for the rights and freedoms of individuals," and that, therefore, require greater protection. Organisations that fall victim to data breaches face high penalties and fines for breaking this law. Additionally, anti-discrimination legislation in many EU countries also limits the types of information organisations can even collect on employees. For example, in many European countries, it is illegal to keep data about ethnic minorities, and people with disabilities may not want to be counted as such. Furthermore, with the capacities of big data for triangulating and reconfiguring data, there are even doubts about whether individuals' information can remain anonymous in the first place.

The OECD Privacy Framework (OECD, 2013) recommends several principles for the handling of personal data: collection limitation principle, data quality principle, purpose specification principle, use limitation

principle, security safeguards principle, openness principle, individual participation principle, accountability principle. Moreover, the European Union's General Data Protection Regulation came into force in May 2018 and replaced the Data Protection Directive 95/46/EC not only as a means of harmonising data privacy laws across Europe, but of providing a new baseline for protecting and empowering EU citizens in accessing their own data (van Ooijen, Ubaldi and Welby, 2019).

More so than the financial risks, however, employers are additionally concerned about potential losses of employee trust should a data breach occur, or if employees perceive that their privacy has been violated (such as, for example, if the data from their employee survey are being used without their consent, or for purposes they did not agree with). Employers, including public sector organisations, may lose credibility and face difficulties in recruiting top talent, potential retention issues, as well as lower levels of employee satisfaction and engagement.

Lack of analytical skills

Until recently, the HR field did not emphasise quantitative skills, and the majority of HR practitioners did not receive training in HR analytics. Pertinent skills are not only IT-related (i.e. sifting through data, developing and maintaining dashboards, etc.), or statistical (i.e. running regressions), but most importantly around "story-telling". That is, HR analysts should be able to ask the right questions and use data in ways that directly respond to business problems and improved performance. This includes also the ability to develop visually impactful representations of data.

The approach adopted by many organisations until now has been two-fold: intensify training in HR analytics, and recruit data scientists to create cross-functional teams/groups around HR analytics. For example, people management decisions at Google are guided by the powerful "people analytics team", which is made up of social scientists who conduct experimental, survey and archival research to inform people-related business decisions.

In June 2019, the US Office of Personnel Management issued a memorandum recognising the job title for data scientists. In a similar vein, Global Affairs Canada has developed a data analytics training pilot programme as part of its overall data strategy to increase data capacity among employees to make greater use of data in evidence-informed policy making. The UK Civil Service has also initiated a Digital, and Technology Fast Stream to attract and develop personnel with digital skills – including digital scientists – into the public service.

References

Deloitte (2016), *People Analytics in HR*, Deloitte. [8]

Frye, A. et al. (2018), "Employee attrition: What makes an employee quit?", *SMU Data Science Review*, Vol. 1/1, https://scholar.smu.edu/cgi/viewcontent.cgi?article=1010&context=datasciencereview. [6]

Heuvel, S. and T. Bondarouk (2016), "The rise (and fall?) of HR analytics: The future application, value, structure, and system support", *Academy of Management Proceedings*, Vol. 2016/1, http://dx.doi.org/10.1108/JOEPP-03-2017-0022. [11]

Huerta Melchor, O. (2013), "The Government Workforce of the Future: Innovation in Strategic Workforce Planning in OECD Countries", *OECD Working Papers on Public Governance*, No. 21, OECD Publishing, Paris, https://dx.doi.org/10.1787/5k487727gwvb-en. [16]

Korea Ministry of Personnel Management (2018), *Measurement of Innovation with Personnel Management Innovation Diagnosis Indicators*. [1]

Marler, J. and J. Boudreau (2017), "An evidence-based review of HR analytics", *The International Journal of Human Resource Management*, Vol. 28/1, pp. 3-26, http://dx.doi.org/10.1080/09585192.2016.1244699. [4]

OECD (2019), *Inclusive Leadership in the Public Service of New South Wales, Australia*, OECD, Paris. [9]

OECD (2019), *OECD Recommendation of the Council on Public Service Leadership and Capability*, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0445. [2]

OECD (2017), *Government at a Glance 2017*, OECD Publishing, Paris, https://dx.doi.org/10.1787/gov_glance-2017-en. [12]

OECD (2016), *Engaging Public Employees for a High-Performing Civil Service*, OECD Public Governance Reviews, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264267190-en. [14]

OECD (2013), *The OECD Privacy Guidelines*, OECD, Paris, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. [7]

OECD (2011), "Strategic human resources management", in *Government at a Glance 2011*, OECD Publishing, Paris, https://dx.doi.org/10.1787/gov_glance-2011-22-en. [15]

Punnoose, R. and A. Pankaj (2016), "Prediction of employee turnover in organizations using machine earning algorithms", *International Journal of Advanced Research in Artificial Intelligence*, Vol. 5/9, pp. 22-26, https://pdfs.semanticscholar.org/fa49/19810eaee67e851ad13775b78c94217a7908.pdf. [5]

Rousseau, D. and E. Barends (2011), "Becoming an evidence-based HR practitioner", *Human Resource Management Journal*, Vol. 21/3, pp. 221-235, http://dx.doi.org/10.1111/j.1748-8583.2011.00173.x. [3]

US Office of Personnel Management (2017), *HRStat Guidance*, US Office of Personnel Management, Washington, DC, https://www.dcpas.osd.mil/content/documents/PA/4_OPM%20HRStat%20Guidance%20June%20%202017.pdf. [10]

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. [13]

OECD Digital Government Studies

The Path to Becoming a Data-Driven Public Sector

Twenty-first century governments must keep pace with the expectations of their citizens and deliver on the promise of the digital age. Data-driven approaches are particularly effective for meeting those expectations and rethinking the way governments and citizens interact. This report highlights the important role data can play in creating conditions that improve public services, increase the effectiveness of public spending and inform ethical and privacy considerations. It presents a data-driven public sector framework that can help countries or organisations assess the elements needed for using data to make better-informed decisions across public sectors.

This publication is a contribution to the OECD Going Digital project which aims to provide policymakers with the tools they need to help their economies and societies prosper in an increasingly digital and data-driven world.

For more information, visit ***www.oecd.org/going-digital***

#GoingDigital

Consult this publication on line at ***https://doi.org/10.1787/059814a7-en***.

This work is published on the OECD iLibrary, which gathers all OECD books, periodicals and statistical databases. Visit ***www.oecd-ilibrary.org*** for more information.

ISBN 978-92-64-51795-0

OECD publishing
www.oecd.org/publishing