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

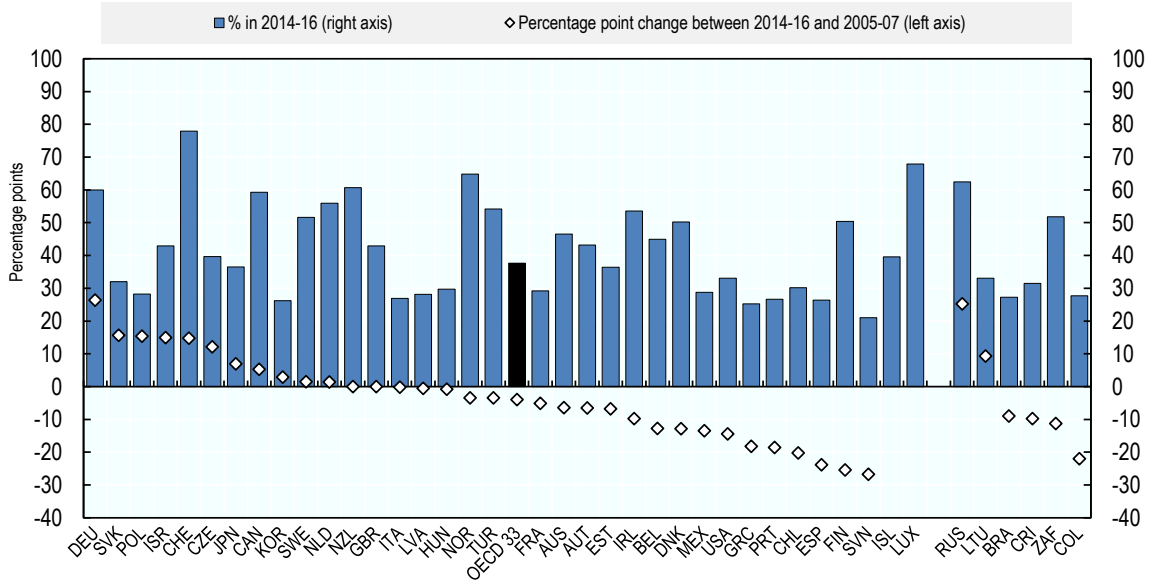
Trust has been defined in several ways by different researchers (McKnight and Chervany, 2000[1]). In this chapter, the word "trust" will refer to "a person's belief that another person or institution will act consistently with their expectations of positive behaviour", based on OECD (2017[2]).

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

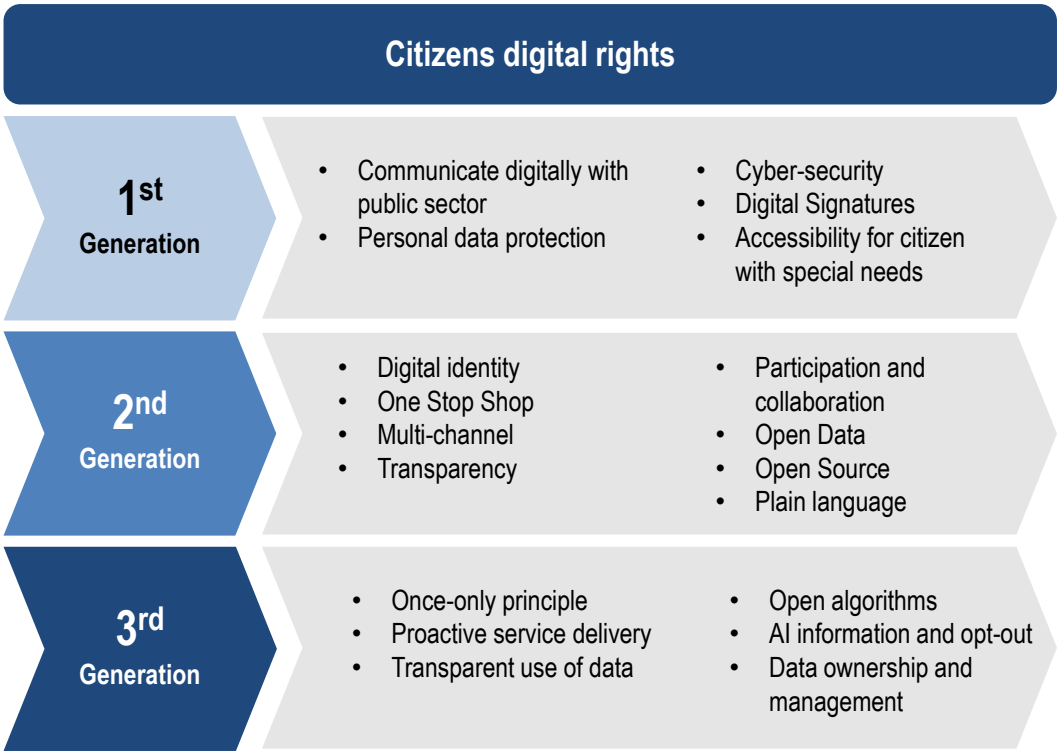
Source: New Zealand Ministry of Foreign Affairs and Trade (2019[13]), Christchurch Call, https://www.christchurchcall.com/call.html.

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]