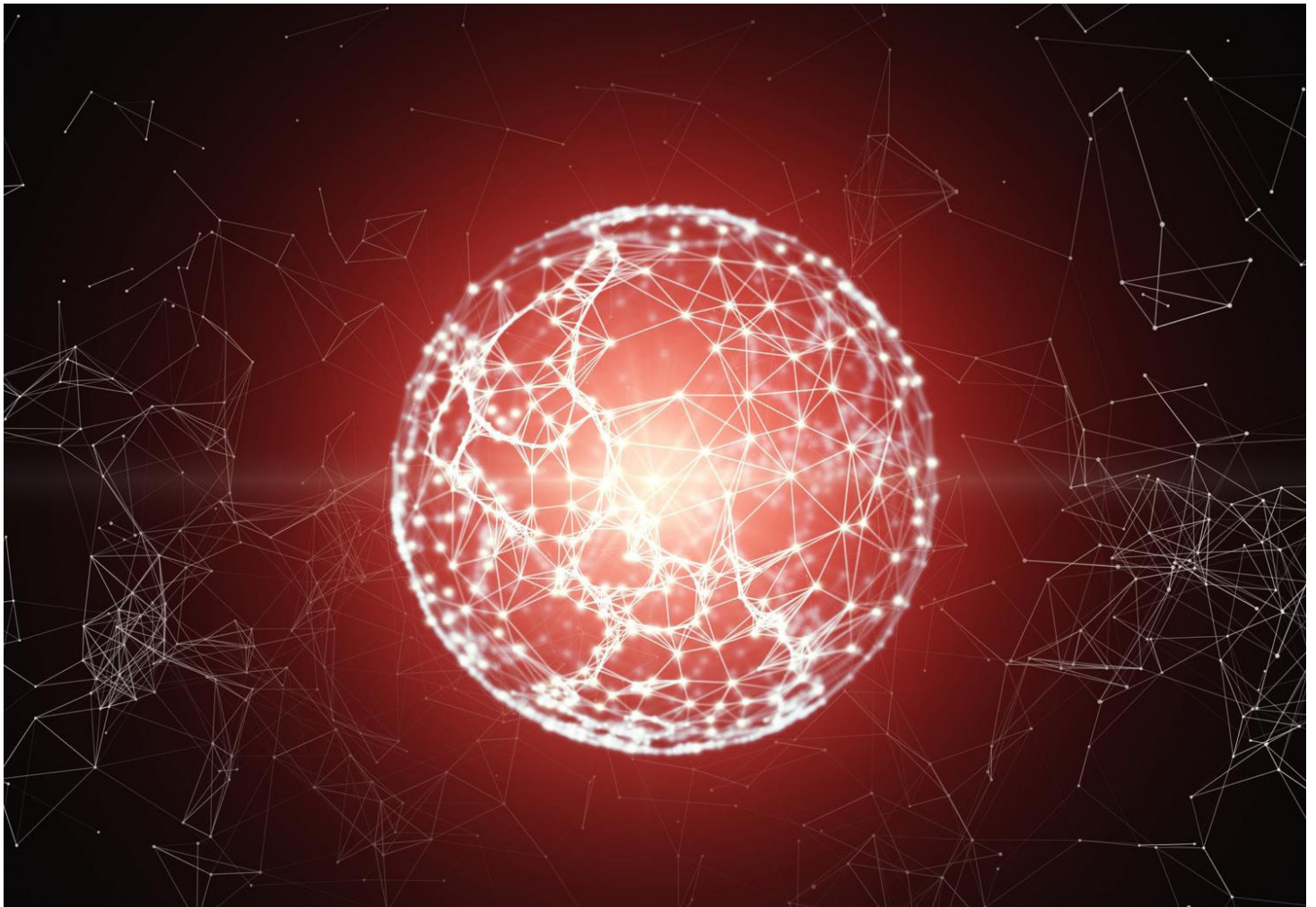


# Data Policy in the Fourth Industrial Revolution: Insights on personal data

Prepared in collaboration with the  
Ministry of Cabinet Affairs and the Future, United Arab Emirates

November 2018



## About the World Economic Forum

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation. The Forum engages the foremost business, political and other leaders of society to shape global, regional and industry agendas.

## World Economic Forum

91-93 route de la Capite  
CH-1223 Cologny/Geneva  
Switzerland



Creative Commons License

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

World Economic Forum®

© 2018 – All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.

# Contents

Preface by the World Economic Forum	4
Foreword by the United Arab Emirates	5
Executive Summary	6
The Data Landscape: making room for complexity and strengthening trust	7
Privacy, data protection and security	8
The need for shared taxonomies	9
Revisiting the Fair Information Practice Principles	10
Defining trust and closing the gap	10
Embracing complexity	11
Context matters	11
Data Policy Response: moving towards outcomes	13
The role of risk-based approaches	13
Managing risk to magnify benefit	14
Sensitive data	15
Vulnerable populations and adverse consequences	15
Conclusion	17
Contributors	18
Endnotes	19

# Preface by the World Economic Forum

**Richard Samans,**  
Managing Director,  
Head of Policy and  
Institutional Impact at  
the World Economic  
Forum

**Anne Toth,**  
Head of Data Policy  
and member of the  
Leadership Team,  
World Economic  
Forum Centre for  
the Fourth Industrial  
Revolution

The digital technologies of the Fourth Industrial Revolution are fast becoming the engine of change throughout all sectors of the global economy. By redefining the manner in which industries, individuals, institutions and governments all interact, the Fourth Industrial Revolution holds unique promise in creating a more inclusive, innovative and resilient society.

The now frequently heard metaphor that “Data is the new oil” acknowledges the important role of data as a fuel for technology and innovation. At the World Economic Forum, we prefer to think of data as the oxygen that fuels the fire of the Fourth Industrial Revolution. It is readily available and necessary, but if used improperly it can generate dangerous and unwelcome results.

As national government and authorities at the subnational level are increasingly concerned with regulating data, new approaches are needed to consider the impact of government regulation and policy-making on technologies central to the Fourth Industrial Revolution. Technologies such as artificial intelligence and machine learning, blockchain, connected devices and smart cities, precision medicine – to name just some of our focus areas – present unique challenges that require new interpretations of existing regulation and a new way of developing future-flexible regulatory models that are adaptive and agile.

Balanced, inclusive and accountable data policies will be fundamental in addressing the growing trust concerns seen throughout today's world. The World Economic Forum sits in a unique position to encourage a global discussion on data policy to help leaders reach positive outcomes for individual countries and the global community. The Forum has long supported the view that “a forward-looking regulatory and legal environment is a vital enabler for bringing new digital services to market in a timely and concerted manner”.<sup>1</sup>

This paper is the first step in what we expect will be a multipronged project designed to help leaders understand the complex dynamics and difficult decisions they will face in managing their transition into the digital domain with respect to personal data and its foundational role. With real-world insights into the implications of effective data policies, the aim is to strengthen their confidence as they create new opportunities while lowering shared risks.

This document advances the notion that forward-looking data policy protocols are critical for a sustainable, inclusive and transparent digital economy. The goal of this report is to contribute to the global discourse on data policy and protection and explore how countries can stimulate rapid advancements in science and technology while minimizing the risks, harms and unintended consequences that may flow from the digital revolution. The objective is not to provide a single set of right answers. Rather, it is to raise the right questions that will help guide policy-makers as they develop effective, predictable and efficient data frameworks that suit their national circumstances.

Leadership from the highest levels of public, private and civic institutions will be vital for these new approaches to take root and have a positive impact. Clarity on how to balance complex and competing interests with transparency, trust and accountability will be essential for sustainable approaches to digital governance. To this end, proactive efforts will be needed to motivate government officials, business leaders and civil society members to establish real-world pilots and to enable continuous and active local engagement with affected user communities.

Investing in an iterative process of multistakeholder dialogue, piloting, experience sharing and refinement is likely to pay dividends for a country's economy over the medium to long term. The Centre for the Fourth Industrial Revolution has been established to support its partners' governments in such processes.

# Foreword by the United Arab Emirates

Ministry of Cabinet  
Affairs and the  
Future, UAE

The 4th Industrial Revolution (4IR) will fundamentally transform key aspects of everyday life through technological transformation. Simply put, the norms and ways in which we do things, as we know them to be, will likely change.

Under the wise leadership of the country, the UAE launched the 4IR Protocol in partnership with the World Economic Forum to establish a regulatory framework of tools and technologies which will drive the next wave of human progress. As an open laboratory for experimentation with advanced technologies, the development of instruments and procedures is crucial in helping governments transition seamlessly towards 4IR technologies. Concurrently, the setting of policies and legislation supports the implementation of novel technologies and addresses new emerging challenges. Last but certainly not least, a key priority of future preparedness relates to an integrated and secure data ecosystem.

In a new context gazing towards the horizon of the exciting future, where change is the only constant, there is a need for robust policy frameworks to govern disruptive trends. This report highlights, inter alia, the importance of an integrated and comprehensive perspective in invigorating data policy responses along such a new era of the 4IR. These include embracing complexity, strengthening trust amongst diverse stakeholders, as well as incorporating risk-based and outcomes-based approaches in addressing data-related perspectives. Along the way, the respect for data privacy underpins the necessity for strong data protection and governance measures across sectors.

This report provides a starting lens in unravelling the complex topic of Data Policy in the Fourth Industrial Revolution. We hope that it will serve as a beneficial impetus to facilitate more thoughts and dialogue.

# Executive Summary

The development of public policy involves trade-offs. The effects of data policy on issues such as technology adoption, economic growth, trade, privacy, security, and other issues should be intentional not accidental.

How policy-makers execute these trade-offs will depend on a wide range of factors, including evolving priorities over time, and the values and ethics rooted in different cultural experiences. No single right answer exists for every country nor is there one bounded set of universal principles. There are, however, commonly accepted, high-level strategic principles that can serve as a starting point.

Important takeaways from this report are:

- There is a need for a common and consistent risk-based framework to help policy-makers identify and understand objective privacy risks to individuals. This does not predetermine policy choices with respect to risk mitigation.
- Stakeholders should frequently and regularly evaluate the context for the intended use of data and the purpose for which it is collected, created, stored, used, processed, disclosed or disseminated.
- Meaningful accountability and consistent enforcement mechanisms are essential for any effective data protection framework and strategy.
- The Fair Information Practice Principles (FIPPs) remain conceptually relevant but need to be adapted to the rapid technological change of the Fourth Industrial Revolution. Innovative technologies will support different applications of the FIPPs and will require frequent reassessment as technology evolves.
- The building blocks to trust are similar to – but different from – FIPPs. Trust must be fostered for data to be used effectively towards innovation. Overall, trust is at a low ebb in most countries surveyed. Effective data policy plays an important role in bridging the current gap.
- The private sector and governments must provide guardrails to help address and minimize harms to build a culture of trust, but must also use policy-making to support the appropriate and beneficial uses of data.
- Security should not be an afterthought when rapid development and deployment of initiatives is taking place. Policy-makers must create incentives for, and reward, strong security as part of technology innovation while recognizing that privacy and security are not synonymous.

- Diverse stakeholders representing different perspectives should be included in the policy-making process – including governments, business, academia and civil society. The common objective should be to harness data for the common good.
- New governance structures are needed to manage digital transformation and to protect digital infrastructure, services and data.
- New frameworks must be able to address the wide range of digital products, services and platforms that exist today as well as services yet to be developed. Policy-makers must understand that ambiguity can lead to lack of flexibility and uncertainty.

This report calls for continued emphasis on outcome-based policy approaches that focus on measurable results rather than rigid compliance checklists. It also calls for ongoing engagement in multistakeholder dialogue and the sharing of knowledge on national data policy through use-cases that can inform and guide leaders in an array of emerging data-protection challenges.

With a richer and more nuanced understanding of complex data challenges, leaders will have a better understanding of how to deploy data policy that best supports their technology agenda while engendering trust.



# The Data Landscape: making room for complexity and strengthening trust

The Fourth Industrial Revolution is reshaping industries, blurring geographical boundaries, challenging existing regulatory frameworks and even redefining what it means to be human. Emerging technologies and scientific breakthroughs such as big data analytics, autonomous vehicles, the Internet of Things (IoT), distributed ledger technology and precision medicine are fundamentally altering the way we live, work and relate to one another. These advancements promise to help countries boost economic growth, create jobs, reduce poverty, promote trade and improve the quality of people's lives.

However, the same technologies that can be used to improve health and medicine, enable personal interaction and engagement and streamline the way governments provide services can also be used to limit access to information, justify discrimination, restrict opportunity and magnify an array of other harmful practices.

At the centre of this broad digital transformation is data. Data is collected, created, used, processed, analysed, shared, transferred, copied and stored in unprecedented ways and at an extraordinary speed and volume. By 2020, an estimated 50 billion devices will be wirelessly connected to the internet.<sup>2</sup>

As billions of sensors come online that passively collect data (without individuals being aware of it) and as computer analytics generate and synthesize more “bits about bits”, understanding how data is generated and how engaged the individual is in its creation has become essential for balance and effective governance. Whether data is volunteered by individuals, observed from behaviour, inferred by organizations or obtained from third parties, the collection, creation, processing and sharing of unprecedented volumes of data is inevitable.

The global regulatory landscape for data is increasingly complex and the net effect of this patchwork quilt of regulation is still unclear. At present, there are more than 120 different national laws governing the collection and use of data, with new laws imminent in the European Union, China and Brazil. Set to go into effect in 2020, a new data-protection law was recently passed in California, the home state of many major technology companies, and national privacy law is now being seriously contemplated in the United States. It's important to note the potential impact of conflicting regulation and data-localization requirements on digital trade and commerce, which is reliant upon cross-border data flows and which helps distribute economic benefits across the globe.

This complexity cannot be “fixed”; it should be taken as a necessary condition of the global modern age and we can expect more of it, not less.

While regulators around the world are experimenting with new approaches to data policy, they struggle with how to address recent technologies that fall outside existing regulatory frameworks. The pace of technological advances means that existing laws and regulations can quickly become obsolete, frustrating both customers and businesses seeking to access new innovations. However, individuals can also become concerned if they feel governments are not sufficiently protecting them from new risks.



## The unique challenges of data policies<sup>3</sup>

Several characteristics of personal data make establishing rules and frameworks uniquely challenging:

- The intangible nature of personal data means it can be copied infinitely and distributed globally, thereby eliminating many of the physical barriers that exist for the trade of tangible goods.
- Data, unlike most tangible assets, is not consumed when used; it can be reused to generate value.
- Data grows ever more connected and valuable with use. Connecting two pieces of data creates another piece of data and, with it, new potential opportunities (as well as new potential harms).
- The role of the individual is changing. Individuals are no longer primarily passive data subjects. They are also increasingly the creators of data. In addition, personal data is intimately linked with an individual's background and identity, unlike interchangeable commodities or goods.

# Privacy, data protection and security

Against this backdrop, a range of issues and concerns frames the modern privacy debate, which raises ethical, technological, legal, economic, cultural and even philosophical questions. The complexity of the challenges does not mean that solutions can't be developed. It does mean that the solutions are unlikely to be simple and straightforward.

The confusion and tension surrounding the issue of privacy arise from multiple directions:

- Semantics of privacy: privacy conveys a variety of overlapping harms, including, for example, the appropriation of a person's picture or name for commercial advantage, surveillance of individual affairs and public disclosure of private facts.
- Power asymmetries: attempting to understand complex and inscrutable data flows within many global platforms is increasingly impractical. It is difficult to measure the value and consequences of different uses of data throughout the value-and-supply chain.
- Macro approaches to privacy: jurisdictions, countries and cultures take different approaches to address the identified harms without any coordinated global policy approach.
- Micro perceptions of privacy: individuals display a range of inconsistent behaviours driven by individual choice and economic rationales, often saying one thing and doing another.

New approaches are needed to help policy-makers address this complexity and to understand, navigate and simplify the challenges. Policy protocols must be considered together to understand how each decision interacts with, or influences, other decisions within a single data policy framework.

Despite the complexity within any given environment, the notion of privacy – the right to private life, data protection and confidentiality of communications – remains highly relevant and affects many other facets of society. A wide range of values and cultural norms inform the way that data policies manifest themselves in daily life. The characterization of privacy as a right necessarily implicates a range of values and norms that may vary from country to country. A country that places less emphasis on individual autonomy may not value

“the right to privacy” to the same extent as other nations, particularly with respect to the relationship between the individual and the state. This becomes directly relevant and influences concrete outcomes when crafting data policies that relate to different harms, including the threshold determination of whether certain harms will be recognized at all.

Different countries place varying levels of priority on the threshold of free flows of information. Similarly, the use of information to discriminate against certain groups is not always a universal concern. The question of which groups should merit protection from discrimination is not shared across the globe and privacy law won't resolve that disagreement.



**One of the greatest individual challenges posed by new information technologies is privacy. We instinctively understand why it is so essential, yet the tracking and sharing of information about us is a crucial part of the new connectivity. Debates about fundamental issues such as the impact on our inner lives and of the loss of control over our data will only intensify in the years ahead.”<sup>6</sup>**



**Klaus Schwab**  
*Founder and Chairman,  
World Economic Forum*

A clear and cohesive data protection framework will provide commercial actors with regulatory certainty, clarify what practices are likely to trigger enforcement or intervention in a given jurisdiction, and make a country's companies, products, services and other potential exports more competitive internationally. As policy-makers work to strike a balance between protecting individuals while also encouraging

---

## Privacy definition

The right to privacy is referenced in the constitutions of over 150 different countries. This notion of privacy is based on the protection of individual privacy and focuses on “individuals’ ability to make autonomous life choices without outside interference or intimidation” and “offers protection against outside intrusion into people’s

homes, communications, opinions, beliefs and identities”.<sup>4</sup>

Data protection – the right to have information about oneself processed fairly – is not the same as the right to privacy. Data protection addresses concerns that information will be incorrectly associated with a person or that inaccurate data will be used to

make a decision about a person. The focus, in this regard, is on the proper and responsible collection, creation, use, processing, sharing, transfer, disclosure, storage, security, retention and disposal of information about people. “This includes decisions by entities about when not to collect, not to create, not to transfer and not to permit.”<sup>5</sup>



# The Fair Information Practice Principles

A paraphrased overview of the FIPPs:<sup>8</sup>



**Collection Limitation:** There should be limits to the collection of personal data relative to its use.



**Use Limitation:** Personal data should not be used or shared for purposes other than those specified in accordance with the purpose for which it was collected, except with consent or as required by law.



**Individual Participation:** An individual should have the right to know what data about them is held by a data controller and to update or erase such information, subject to reasonable restrictions.



**Data Quality:** Personal data should be relevant to the purposes for which it is to be used, and should be accurate and up to date.



**Security:** Personal data should be protected by reasonable security safeguards.



**Accountability:** A data controller should be accountable for complying with measures that give effect to the principles above.



**Purpose Specification:** The purposes for which personal data is collected should be specified at the time of collection and its use should be consistent with the stated purpose.



**Openness:** There should be a general policy of openness about developments, practices and policies with respect to personal data.

innovation and growth, the uncertainty and instability this creates will vary among stakeholder communities. Policies that are flexible, iterative and adaptive can address some of the differing stakeholder perspectives.

Along with the distinction between privacy and data protection, the relationship between privacy and security also warrants clarification. These two terms are overlapping and complementary, but they are foundationally different. Information security concerns the confidentiality, integrity and availability of information. Privacy risks may result from authorized activity that is beyond the scope of information security. Thus, protecting individuals' privacy cannot be achieved solely by securing personal data. Security involves protecting information from unauthorized access, use, disclosure, disruption, modification or destruction.

Privacy, on the other hand, is concerned with managing the risks to individuals associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure or disposal of personal data.

## The need for shared taxonomies

The word "privacy" has different meanings to different people, and slight variations in meaning exist among different languages. Stakeholders often subtly change the definition or use of a word to reflect their own values, promote a specific

interest or direct a policy debate towards a particular outcome. Many of the core terms, the word privacy in particular, are vague and imprecise and often lead to an inchoate public conversation built upon a "fog of data ignorance".<sup>7</sup> A more precise use of language is overdue.

While the call for better and more precise taxonomies is not new, the growing public debate on how data is being used points to an increased need for a more constructive dialogue.

Shared taxonomies on the nature of digital trust, the differences in data origin, what constitutes personal data and the types of data harms are just some of the areas where a more precise, structured and defined conversation would drive meaningful progress. Adopting common taxonomies can help stakeholders align on shared understandings of both the quantitative change in the amount of personal data being created as well as the qualitative differences based upon how it originated.

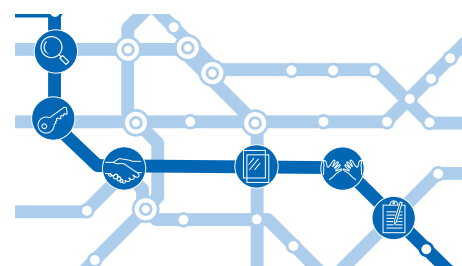
Industry, government and citizens frequently disagree on these central points of discussion. Yet without a shared taxonomy of those terms, it will be impossible to have a productive discussion on how to collectively govern and regulate data flows.

With more widely aligned taxonomies, the "inputs" into the policy-making decision processes can be made more

## Complexity is neither vague nor ambiguous

Complexity should not be confused with ambiguity and vagueness. Ambiguity occurs when words can be interpreted in more than one way. Vagueness is when words are not clear and there is doubt about the intended

meaning. For intended outcomes to be achieved, a complex regulatory framework needs text that is clear, precise, unambiguous and properly integrated into a country's larger legal regime.



consistent. This, in turn, will encourage a more productive dialogue and help identify the reasons behind variations in approaches. It may also serve to illustrate how different data policy frameworks actually share far more in common than previously understood.

## Revisiting the Fair Information Practice Principles

An early attempt at developing a shared vocabulary and a common set of principles saw the publication of the Fair Information Practice Principles (FIPPs) nearly 40 years ago. The FIPPs are the basis of most privacy laws and data-protection frameworks in effect today. They represent stable, high-level principles that are meant to be scalable and adaptable.

There is no doubt, however, that the FIPPs require further consideration and refinement. As machine learning and artificial intelligence (AI) find new ways to leverage data in larger volumes, the question of data-minimization thresholds and limits on usage become important to revisit given the potential for advanced analytics to deliver an array of transformative outcomes (both benefits and harms). With new forms of ubiquitous and ambient data collection through IoT and connected devices, models of consent must change and adapt. There are many other examples where traditional interpretations of the FIPPs are strained when faced with new technologies.

Reinterpreting the FIPPs, or simply evaluating them in light of new technologies, may serve to effectively modernize any FIPPs-based regulation currently in effect. Like shared taxonomies, a better and shared understanding of how the FIPPs apply to the disruptive technologies of the Fourth Industrial Revolution may provide additional commonalities in approaches already underway.

## Defining trust and closing the gap

Another barrier we see that may hinder rapid adoption of the technologies of the Fourth Industrial Revolution is the recent widening of the trust gap across the world.

The widespread trust concerns within the digital ecosystem during the past few years are unmistakable. Security breaches, identity theft and fraud; concern from individuals and organizations about the accuracy and use of personal data; companies confused about what they can and cannot do; and increasing attention and sanctions from regulators are just some of the indicators. In fact, in 2017, the global Edelman Trust Barometer had its biggest drop in trust ever<sup>9</sup> across the institutions surveyed of government, business, media and NGOs compared to the previous year. In 2018, though outliers to this trend persist, little had improved and some important markers were even worse.<sup>10</sup>

Moving forward on the issue of trust will require a more defined and structured conversation. The World Economic Forum has identified six essential principles for ensuring a trustworthy data system. All of these dimensions are highly interconnected and each brings a unique set of opportunities for data policy-makers.<sup>11</sup>

## The six dimensions of trust



### Security

Operating on shared technical infrastructure, the confidentiality, integrity and availability of both data at rest and data in motion are critical given their increasingly granular, real-time and valuable nature.

### Accountability

The use of data (and the platforms which enable its use) must function as promised; stakeholders must comply with legal requirements and agreed-upon processes and be held responsible in the event of system failure.

### Transparency

Individuals need meaningful ways to understand and decide on how their data is to be collected, stored, processed and shared. They also need to have a functional and active relationship with the entities that hold and process their data so that the intent and desired outcomes of these entities can be better understood.

### Auditability

The systems that use data must have the capacity to be externally audited and verified, and policy-makers, in many instances, lack the robust means to audit data regulations given the velocity, global nature and complexity of the underlying technical architectures.

### Fairness

Regulators and data-protection authorities need to be increasingly vigilant about both privacy abuses and an array of other harms (economic, social and political).

### Ethics

Unethical (or even illegal) use of data can permanently damage trust among stakeholders.

It is widely believed that trust is essential for a sustainable, inclusive, innovative and trustworthy digital ecosystem to emerge. The extent to which a country maintains an effective, predictable and efficient data-protection framework will be evaluated by multiple stakeholders. How a data protection framework is implemented and enforced will affect each of these relationships. It remains as true today as ever that trust is difficult to gain and easy to lose. It is incumbent upon policy-makers to develop an environment of trust if data is to be used for maximum benefit.

## Embracing complexity

Along with the policy concerns across the various dimensions of trust, another foundational factor is the complexity and velocity of the global data ecosystem, and the technology that enables it. With rapidly growing data volumes, increasingly trans-border data flows, the increasingly granular and real-time nature of connected device data, the inscrutable nature of AI systems and the growing concentration of global platforms, policy-makers are facing an unprecedented set of known (and unknown) emerging risks. Data policy-makers need to embrace this complexity and invest in resources to understand and manage it – not ignore it.

Embracing the complexity of the Fourth Industrial Revolution demands a variety of appropriate responses. It may not be obvious, but the same amount of effort, rigorous analysis and resources are required to develop a data protection framework that seeks to achieve a high level of privacy protection as it does to form a framework designed to be more permissive and less protective. In both cases, policy-makers must understand the full range of benefits, risks, desired outcomes and potential unintended consequences of a given framework. Decisions in either direction should be fully informed, carefully crafted and deliberate. In some instances, it may call for more open, experimental and rapid innovation. In other contexts, it may mean more deliberative and considered approaches that may slow the pace of innovation while creating an environment where stakeholder trust is nurtured, and where individuals more readily accept new technology.

As it relates to data policy, one clear reality is that the complexity of the data ecosystem means policy frameworks built around bright-line tests and rules won't have the agility, resilience or support of users. While clearly defined rules may simplify compliance in terms of what is permissible (and what is prohibited), they may not be sustainable. Alternatively, those same, equally clear bright lines could prevent adverse consequences but constrain innovation. This is why an outcome-based approach is necessary.

Further complicating the appropriateness of responses, making public-sector information available can be a means of encouraging public engagement and supporting innovative uses of data. This represents a transformation from a logic of government transparency and freedom of information to that of enabling analytical uses of data.

## Context matters

In an environment of such complex dynamics, one of the other foundational factors is the importance of context. In many ways, data policy has entered a world of "it depends". It has become too difficult to adequately assess the sensitivity of a given data element or dataset without considering its context. What is sensitive data in one context will change over time, particularly as technology creates new methods of identification and authentication. Additionally, the value and/or sensitivity of a given piece of data will change as it is combined and analysed to create inferences.

A more nuanced way to think about the issues of data policy requires a contextual mindset based on the origin of the data collection, the data sensitivity and the intended uses. Putting aside the challenges of data security for a moment, focusing on the contextual dependencies of data begins to raise questions about how shared rights, responsibilities and appropriate permissions can be established for data to flow in ways that both ensure the integrity of a given context and balance the interests of relevant stakeholders.

One important dimension shaping the data ecosystem can be seen along the continuum of how personal data originates. We need to consider data sources and methods. Data that

## The importance of context

Assessing risk requires those setting policies to consider the context in which data is collected and processed.

Relevant considerations include:




- Source of the information – the information could be collected directly from the individual, from other individuals or entities, or from publicly available sources.
- Collection method – the information could be acquired from sensors inside an individual's

home, CCTV in public spaces, DNA from a bio sample, or a wearable health monitor.

- Private or public facts – the information may have been made available, shared or publicly posted by the individual or the information may have been intended to remain private.
- The entity – the entity collecting the data may be a government or law enforcement agency, a commercial actor, a charity or an educational or medical institution.

- Individuals' relationship with the entity – the data may be processed by a known entity with whom the individual has an ongoing commercial relationship or an unknown third party
- Intended use of the information – was the data used as agreed and contemplated by the individual or was the individual surprised?
- Sensitivity of the information – the personal data may be related to sensitive issues such as health or common commercial activities.

# How data originates impacts its relational dynamics

Type	Example
Individually provided	 <ul style="list-style-type: none"><li>Photos</li><li>Blogs</li><li>Emails</li><li>Tweets</li><li>Online transaction details</li><li>Registration forms</li><li>Job applications</li></ul>
Observed	 <ul style="list-style-type: none"><li>Internet browsing preferences</li><li>Surveillance video</li><li>Location data</li><li>Call detail records</li></ul>
Inferred	 <ul style="list-style-type: none"><li>Credit scores</li><li>Consumer profiles</li><li>Predictive traffic flows</li><li>Patterns in the spread of infectious diseases</li><li>Targeted advertisement</li></ul>

is volunteered by individuals, data that is observed about individuals and data that is inferred about individuals each have different relational dynamics in terms of perceived senses of control and ownership.

Moving along the spectrum – from individually provided to observed and finally to inferred data – organizations tend to feel an increased sense of ownership and control, particularly as the time, energy and financial resources devoted to creating it increases. There are generally few incentives for organizations to share observed or inferred data either with individuals or with competitors.<sup>12</sup>

At the same time, the perceived privacy harms increase as individuals lose a sense of control over how the granular and predictive insights related to them are being used. The more distant data gets from the awareness of an individual and the more intimate and predictive it becomes, the greater the sense of unease and suspicion. This aspect, this loss of control and sense of intrusion, is one of the factor where the context for how the data was collected and how it is being used needs to be comprehensively addressed. The impact of harm is subjective in these variable scenarios.

Faced with the challenges of updating the FIPPs, managing complexity and addressing context, a new model for data policy that encourages continued innovation in the Fourth Industrial Revolution needs to be developed.





# Data Policy Response: moving towards outcomes

Given the complexity, context-dependency and the growing need for trust in today's global digital economy, how do we move forward? While still in its early stages of development, an outcome-based approach to data policy holds promise.

Outcome-based approaches provide the means to balance competing tensions in a globally interoperable way. They can help countries develop not only effective data-protection frameworks but also deploy those that can be implemented in different regions across the globe. Outcome-based approaches are unique in their ability to allow for regional and local differences while supporting the autonomy of local actors. It is inevitable that data-protection frameworks will diverge given the different legal regimes, government institutions and economic models among various countries and even cities. The inconsistencies in these approaches often have less to do with views on privacy and more to do with differences in culture and values.

Helping countries harmonize regulatory approaches to privacy and data protection can also serve to reduce digital-policy fragmentation around the world, which often impedes global trade, cross-border data flows and international collaboration. The free flow of trustworthy data is essential for innovation and for the potential benefits of advancements in technology to reach their full potential.

It is also worth noting that some aspects of global harmonization of data policy frameworks may not be a universally shared objective. Some countries may affirmatively object to harmonization efforts and knowingly implement requirements that are incompatible in certain specific respects with other regimes. Data-localization requirements are one

such policy option that are designed to meet a local need where interoperability is not the primary policy objective. That may be a valid and rational outcome for a given country if the decisions are made deliberately and with a full appreciation of the implications for other governmental, commercial and civil actors.

## The role of risk-based approaches

The broader adoption of the discipline of risk management and the use of risk-based impact assessments are critical to the implementation of outcome-based approaches. There is now a consensus that risk management has an increasingly important role to play in 21st-century data protection regimes. The use of privacy risk assessments is now a part of frameworks in the United States, Australia, New Zealand, Canada and the European Union. Within the EU, its General Data Protection Regulation (GDPR) mentions the word “risk” 75 times. Regardless of which specific methodology is employed, resources, careful analysis and judgement are required to implement the risk framework and apply the lessons to policy decisions and regulations.

One of the main benefits of using risk-based approaches is that they can enable desired outcomes to be achieved and are therefore compatible with outcome-based frameworks. With risk-based assessments in place, the decisions of policy-makers are more fully informed and do not represent one stakeholder's interests to the exclusion of others. Absent the use of risk-based approaches, when there is no link between data requirements and the likelihood of a material impact occurring, and the result can be a disproportionate

---

## Outcome-based approaches

An outcome-based approach seeks to measure organizations against whether they have achieved a desired policy outcome rather than measure compliance against a fixed checklist.

A benefit of an outcome-based approach is that it recognizes that the same outcome, or better outcomes, may be achieved by allowing flexibility in the process. It is also very compatible with risk-

based frameworks because they are, by definition, variable and can be better served by approaches that are not rigidly fixed. Perhaps the most important benefit of an outcome-based approach is that it is a model designed for interoperability. In the global context, this allows for regional variation in how an outcome is achieved, enabling different nations to determine approaches that suit them individually.

One challenge of an outcome-based approach is that measuring “success” against a stated outcome may be more difficult from an auditability standpoint as the process by which it is achieved is not standardized. It also may offer less certainty to organizations seeking assurances that their approach has met some minimum threshold for compliance.



emphasis on procedural, tick-the-box data policy compliance.

Implementing risk-based approaches is not easy or inexpensive. Embracing risk means going well beyond legal compliance and embracing rigorous analysis, deliberation and, at times, confronting issues of ethical uncertainty. The aim is to fully inform decision-makers on potential risks, so they aren't intentionally, or accidentally, ignored. The process is designed to render decisions that are informed, deliberate and human.

After the various assessments and decisions have been made, there are generally three potential outcomes:

1. Decision-makers agree the initiative has a high probability that a material set of adverse consequences could occur, so the initiative is terminated regardless of the potential benefits.
2. Decision-makers consider all of the potential risks and decide that the initiative will go forward as proposed. No changes to mitigate risk are taken as the risks are viewed as insignificant or the potential benefits outweigh the risks.
3. Decision-makers take some steps to mitigate some risk and the project goes forward with full knowledge and acceptance of any residual risks.

The area of privacy provides a clear example of where risk-based approaches can serve to navigate the complexities of data policies. A narrowly tailored, limited data-protection framework that focuses on risk and outcomes rather than mechanical procedures may in fact have more impact than a sweeping framework that requires a rigid set of procedural requirements.

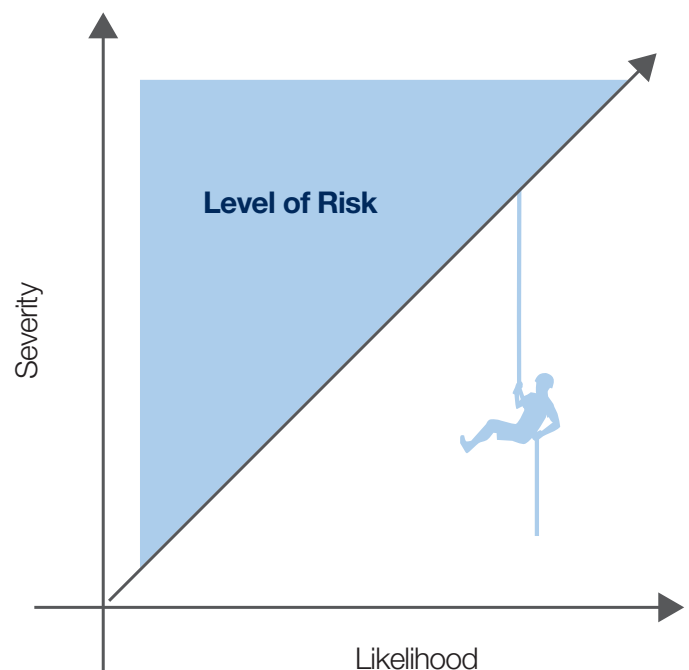
Risk-based approaches embrace the contextual dependencies of the data economy and enable both individuals and policy-makers to understand more fully the consequences of the effect of one change on stakeholders at the individual level as well as on the larger ecosystem. By enabling policy-makers to focus on the risks of harm at the individual level, the analysis of privacy policies can be viewed through the eyes of the individual and outcomes can be more human-centred and inclusive.

Addressing the complex dynamics of the modern data ecosystem, risk-based approaches also serve to easily identify unintended policy consequences and highlight where negative cascading effects could occur.

## The risk lifecycle



## The relationship between severity, likelihood and the level of risk



## Risk assessment: focusing on the smart questions to ask

The use of data risk-assessment tools can serve policy-makers in their core mission: making good decisions. Continually asking these questions can be of great utility:

- “What is the problem we are trying to solve through regulation?”
- “What is the ‘it’ that we are seeking to prevent through regulation?”
- “What is the desired outcome we want to achieve through regulation?”

# The risks of personally identifiable information and the Fourth Industrial Revolution

Personally identifiable information (PII), historically referred to a relatively narrow range of data such as name, address, birth date, Social Security or government ID number and financial information such as credit card numbers or bank accounts. But this is changing in some contexts as leaders acknowledge that a bright-line definition is neither possible nor desirable given the advances in data science and technology.

Many legal frameworks have traditionally viewed data in a binary manner: data was either personally identifiable, and therefore covered by a framework, or it was de-identified and thereby outside the framework.

This approach had the perceived advantage of making compliance for business straightforward, depending upon the breadth and scope of the definition of “personally identifiable”.

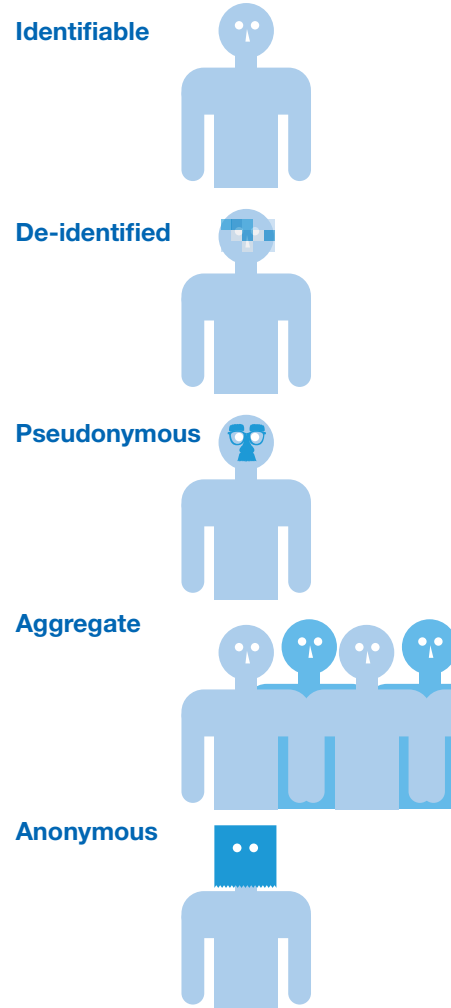
Yet as technology evolves, data that was once thought to be difficult to identify has become easier, less expensive and less resource intensive. Increasingly, data policy frameworks

reflect today's reality and embrace the notion that the identifiability of data (or a dataset) exists along a continuum.

Various data protection frameworks incorporate this continuum in concepts such as:

- Identifiable data
- De-identified data
- Pseudonymous data
- Aggregate data
- Anonymous data.

This requires an assessment of the risk of identifiability (or re-identifiability), which is an evolving concept. De-identification should not be viewed as the solution to issues related to data protection and privacy, but as one tool that can be used to mitigate risk in the larger context of a comprehensive data protection framework.



## Managing risk to magnify benefit

Risk-based data-protection policies can serve to encourage increased innovation and investment as they provide the foundation for a more predictable and reliable digital ecosystem to flourish. The risk-based approach, for example, reduces obstacles to the development of new technologies, such as blockchain. Indeed, distributed-ledger technologies are often impaired by strict data protection requirements that do not take consumer harm into consideration, focusing instead on a checklist approach. Policy decisions on the appropriate steps to manage a given risk (within a given context) require a deeper comprehension of the impact on commercial interests, and the incentives to invest over time can be better understood.

The use of risk-based approaches requires a continuous commitment to evaluate and revisit previous data policy decisions. Risks will change over time. Risk-based policy-making is an ongoing process, not a one-time exercise. Implicit in undertaking a risk-based approach is the understanding that the goal of managing risk is maximizing benefit. The risks to be balanced relate to sensitivity of data, vulnerability of populations and possibilities of adverse consequences.

## Sensitive data

Identifying and setting specific rules for categories of sensitive data is now a core part of nearly every data protection framework. Over 75 countries have defined sensitive data or classified special categories of personal data. This recognizes that different data elements (or categories of personal data) present different levels of risks to individuals.

Whether or not a given dataset is labelled as personal or not, the more relevant analysis is the sensitivity of the data in a given context and the potential risk of adverse consequences or harms to individuals from the processing of that data. What is considered sensitive is often subjective and may vary from country to country, based on cultural, historical and other factors.

Understanding the sensitivity of a data element, or given category, is important not only in the context of privacy but for data security, information governance and risk management more generally. Once categories of sensitive data are identified, a framework must identify the implications of being labelled as such within a given framework. Higher standards regarding consent, security and legitimate use may be appropriate. In some cases, the collection and use of certain sensitive information may be prohibited outright.

## Common categories of sensitive data

While definitions of “sensitive data” vary by country and region, the following categories appear frequently:

- Information about physical and mental health
- Information revealing racial or ethnic origin
- Religious beliefs or affiliations
- Criminal records
- Political, philosophical or other personal views or orientation
- Trade union or political party affiliation
- Unique identifiers used in financial transactions
- Genetic information
- Information from (or about) children under the age of 13
- Precise location information over time

## Vulnerable populations and adverse or unintended consequences

In the use of risk-assessment tools, the question of “risks to whom” also warrants special consideration. Risks seldom affect the different communities within a country or region equally. Just as a different level of protection may be advisable to protect sensitive personal data, different policies or standards may be advisable for certain population segments. For example, genomic data can reveal sensitive health-related insights about individuals and their relatives. Genetic research may therefore identify information that is unique to a specific population segment, potentially subjecting them to discrimination, stigmatization or denial of medical treatment.

Overall, given that vulnerable populations may face a greater risk of adverse consequences than the general public in given contexts, policy-makers should identify populations

that merit a higher level of protection and determine whether specific requirements should be codified within a data-protection framework.

Along with a commitment to establish the organizational agility and capacity to continuously re-evaluate certain data policies, one of the critical first steps is for policy-makers to create a taxonomy of adverse consequences and data-related harms. A near-term priority for stakeholders within the digital ecosystem is to collectively align on what classes of harm should be recognized in a particular framework and how they will be measured. Where a class of known or anticipated harms is not recognized, reasons need to be articulated for not including that harm in a policy decision.

Concretely, this work needs to focus on an initial set of objective problems because: 1. they exist in some form; and 2. there can be a causal link between the problem and the processing of data.

## Adverse consequences beyond privacy

Upholding the notion of privacy is a necessary but insufficient condition for a healthy data ecosystem. These are just some of the adverse consequences that are related to data but fall outside data policy frameworks.



Direct financial loss from fraud, identity theft or other practices



Physical harm to a person including loss of life



Restriction of freedom of movement or travel resulting from incomplete or inaccurate information



Discrimination based on facts or inferences including disparate impact from false, inaccurate or incomplete information



Price discrimination or other negative economic impacts



Health and safety risks including risks to public health



Damage to reputation



Embarrassment, humiliation or emotional distress



# Conclusion

A simple goal of this paper was to debunk the view that data policy choices are binary decisions with clean and clear demarcations. Rather, the point is to embrace the complexity of the Fourth Industrial Revolution. This complexity is manifested not just in the technology itself but in the challenges of a global landscape where different technologies are deployed at different rates in nations with different embedded values, cultural norms and states of economic development, and different development goals.

Because of this complexity, we recommend an outcome-based approach to data policy that focuses not on specific compliance methods but on measurable policy results. This model has the advantage of allowing for and encouraging diverse approaches. This makes it an appealing model to achieve potential global interoperability throughout the 120 plus different existing data protection laws currently in effect across the world.

Above all, trust is an essential foundation for technology adoption and the first and most pressing requirement of data policy. In the world today, trust is increasingly low and must be addressed urgently. The six interconnected foundations of trust -- accountability, ethics, auditability, transparency, fairness, and security -- all must be addressed to help close the gap in trust.

The potential benefits from advancements in technology are extraordinary and transformative. As noted earlier, "the Fourth Industrial Revolution will generate great benefits and big challenges in equal measure." Both must be addressed.

The frameworks articulated in this relatively brief paper are a start to thinking about the complex topic of data policy. There is no one single approach that will suit all stakeholders. Enabling data policy frameworks of the Fourth Industrial Revolution must be both flexible enough to accommodate differences in values and norms as an enabler of technology innovation.

Below is an initial list of areas for further consideration:

- Provide policy makers with uniform, comparable information on data protection frameworks that will give them insight into when and how a proposed framework may diverge from other frameworks, ensuring that fully informed decisions are made before a framework is codified and implemented.
- Address the distinction between privacy and security including an examination of public perception.
- Develop a common understanding and set of criteria for concepts related to identifiability and what is necessary and sufficient to ensure that data is appropriately de-identified.
- Offer an analysis of vulnerable populations across the globe to assist policy makers in providing consistent levels of protection to vulnerable populations.
- Analyze various iterations of the FIPPs (beyond that which the OECD originally published) with an objective of developing a universally recognised set of modernized FIPPs. This may identify the most common principles and highlight additional principles that appear in different contexts.
- Conduct a comprehensive analysis of sensitive categories of personal data to identify those areas that are most commonly considered sensitive across jurisdictions and determine whether those mappings reflect common consumer understanding of sensitivity. We have offered a summary view in this paper. A more thorough examination may be in order.



# Contributors

## The Ministry of Cabinet Affairs and the Future, United Arab Emirates

## The World Economic Forum:

### **Anne Toth**

Member of the Leadership Team – Centre for the Fourth Industrial Revolution, Head of Data Policy

### **William Hoffman**

Project Lead, Data Policy

### **Eddan Katz**

Project Lead, Data Policy

### **Tooba Durraze**

Project Specialist, Centre for the Fourth Industrial Revolution

### **Jesse Lin**

Project Specialist, Centre for the Fourth Industrial Revolution

### **Saverio Puddu**

Fellow, Centre for the Fourth Industrial Revolution

### **Nada Al Saeed**

Fellow, Centre for the Fourth Industrial Revolution

## Acknowledgements

Special thanks to Marc Groman for his time, energy and insights in the writing of this report. His support and commitment were invaluable and deeply appreciated.

Illustrations and layout by Design Resources Ltd.



# Endnotes

1. World Economic Forum, Digital Policy Playbook 2017: Approaches to national data governance (September 2017): [http://www3.weforum.org/docs/White\\_Paper\\_Digital\\_Policy\\_Playbook\\_Approaches\\_National\\_Digital\\_Governance\\_report\\_2017.pdf](http://www3.weforum.org/docs/White_Paper_Digital_Policy_Playbook_Approaches_National_Digital_Governance_report_2017.pdf) (link as of 1/11/2018).
2. Gartner, Gartner Says 8.4 Billion Connected “Things” Will Be In Use in 2017, Up 31 Percent from 2016 (7 February 2017): <https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016> (link as of 1/11/2018).
3. World Economic Forum, Rethinking Personal Data: Strengthening trust, 2012: <https://www.weforum.org/reports/rethinking-personal-data-strengthening-trust> (link as of 31/10/2018).
4. The Constitute Project. Searchable & Comparative World Constitutions: <https://constituteproject.org/> (link as of 31/10/2018).
5. United States National Science and Technology Council (NSTC), Networking and Information Technology Research and Development Program, National Privacy Research Strategy (June 2016): <https://www.nitrd.gov/pubs/NationalPrivacyResearchStrategy.pdf> (link as of 31/10/2018).
6. Klaus Schwab, World Economic Forum: Global Agenda, The Fourth Industrial Revolution: What it means, how to respond (14 January 2016): <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/> (link as of 31/10/2018).
7. David Brin, in Rethinking Personal Data: A new lens for strengthening trust, World Economic Forum 2014: <http://reports.weforum.org/rethinking-personal-data/> (link as of 31/10/2018).
8. Additional information on the FIPPs and their origin through the OECD can be found at <http://oecdprivacy.org/> (link as of 31/10/2018).
9. 2017 Edelman Trust Barometer (21 January 2017): <https://www.edelman.com/research/2017-edelman-trust-barometer> (link as of 31/10/2018).
10. 2018 Edelman Trust Barometer: Global Report: [https://www.edelman.com/sites/g/files/aatuss191/files/2018-10/2018\\_Edelman\\_Trust\\_Barometer\\_Global\\_Report\\_FEB.pdf](https://www.edelman.com/sites/g/files/aatuss191/files/2018-10/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf) (link as of 31/10/2018).
11. World Economic Forum, Digital Transformation Initiative: Unlocking B2B platform value, 2017: <http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/wef-platform-report-final-3-26-17.pdf> (link as of 31/10/2018).
12. World Economic Forum, Rethinking Personal Data: Strengthening trust, 2012.



---

COMMITTED TO  
IMPROVING THE STATE  
OF THE WORLD

---

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

---

World Economic Forum  
91–93 route de la Capite  
CH-1223 Cologny/Geneva  
Switzerland

Tel.: +41 (0) 22 869 1212  
Fax: +41 (0) 22 786 2744

[contact@weforum.org](mailto:contact@weforum.org)  
[www.weforum.org](http://www.weforum.org)