GPA
Global Privacy Assembly

Policy Strategy Working Group 2: Digital Economy

Report – adopted October 2020

Chair: EDPS

globalprivacyassembly.org

Table of Contents

Executive Summary

One of the Strategic Priorities of the GPA for 2019-2021 is to enhance Conference's role and voice in wider digital policy and strengthen relationships with other international bodies and networks advancing data protection and privacy issues, including through observer arrangements.

As part of its Policy Strategy, the GPA decided to develop a narrative on how data protection and privacy regulation provides safeguards for the public and supports trust in the digital economy. Specifically, the GPA aims to "*develop a clearer and broader narrative for a longer-term and more coherent approach to issues around the data protection aspects of regulation of the digital economy, including through closer engagement with relevant multilateral and international bodies.*" (Pillar #3 Action II of the Conference Strategic Direction). Policy Strategy Working Group 2 (PSWG2) was created to deliver the actions around this theme.

Based on this mandate, PSWG2 has developed a **background paper** that explains how data protection and privacy regulation provides safeguards for the public and supports trust in the digital economy. It has also identified **possible next steps to engage more closely with relevant multilateral and international bodies** in order to give the GPA a stronger voice in global debate and initiatives surrounding the digital economy.

PSWG2 **seeks the 2020 Closed Session participants' support for**

- the **adoption and publication** of the **background paper** entitled "*Towards a trustworthy digital economy*";
- the undertaking of **engagement activities** in relation to external stakeholders.

Introduction

- **Mandate and objectives**

The establishment of PSWG2 results from the 2019 Resolution on the Conference's Strategic Direction. The mandate of PSWG2 is to "*develop a clearer and broader narrative for a longer-term and more coherent approach to issues around the data protection aspects of regulation of the digital economy, including through closer engagement with relevant multilateral and international bodies*" (Pillar #3 Action II).[1]

- **Main activities during 2020**

After defining its methodology and work plan, PSWG2 developed a background paper that explains how data protection and privacy regulation provides safeguards for the public and supports trust in the digital economy. It has also identified possible next steps to engage more closely with relevant multilateral and international bodies in order to give the GPA a stronger voice in global debate and initiatives surrounding the digital economy.

PSWG2 met via teleconference four times between February 2020 and July 2020 engaging in addition when required via email.

- **Working group members**

EDPS (Chair)	CNIL France	CNPDCP Gabon	CNPD Luxemburg	NPC Philippines
INAI Mexico	UK ICO	KVKK Turkey	Ministry of Electronics & Information Technology, India (observer)	EDPB (observer)

- **Liaison with the SDSC**

On 18 June 2020, the Chair of PSWG2 participated in the 3rd Meeting of GPA Strategic Direction Sub-Committee. It was agreed that the proposed future engagement activities should also include criteria to evaluate the success of these activities. The success of the proposed engagement activities carried out in 2020-2021 will be measured on the basis of the number of invitations received and/or events in which the GPA is represented following the proposed engagement during this period.

[1] GPA Resolution on the Conference's Strategic Direction 2019-21, Annex p.9.

Working Group Activities

1. Development of background paper: "Towards a trustworthy digital economy"

The background paper explains how data protection and privacy regulation provides safeguards for the public and supports trust in the digital economy. To demonstrate why data protection and privacy regulation are essential for the digital economy, this paper considers the following questions:

- What is the digital economy?
- What are important developments and trends in the digital economy?
- Why are privacy and data protection important in this context?
- How does data protection and privacy regulation benefit individuals, businesses, governments and society as a whole?

The background serves as a basis to develop a longer-term and more coherent approach to issues around the data protection aspects of regulation of the digital economy, including through closer engagement with relevant multilateral and international bodies. For the immediate future, it is proposed that that background paper helps support the engagement efforts towards relevant stakeholders.

2. Preliminary identification of relevant stakeholders

As part of its methodology and work plan, PSWG2 has identified possible next steps to engage more closely with relevant multilateral and international bodies in order to give the GPA a stronger voice in global debate and initiatives surrounding the digital economy. In this context, Workstream 2 has:

- reflected on the approach the GPA should use to promote outputs of the work, engage with stakeholders and influence global discussions;
- identified a number of relevant stakeholders at international level and considered other relevant stakeholders;
- identified specific initiatives the GPA could take and/or contribute in order to increase the visibility and resonance of the work.

The current inclination of PSWG2 is to target stakeholders that bring together policymakers who develop policies with data protection and privacy implications, but do not necessarily have privacy and data protection in the focus of their core mandate.

Forward looking plan 2020-2021

PSWG2 intends to focus on engagement activities with relevant multilateral and international bodies in order to give the GPA a stronger voice in global debate and initiatives surrounding the digital economy, in line with Pillar #3 Action II of the Conference Strategic Direction.

PSWG2 will seek the 2020 Closed Session participants' support for

- the adoption and publication of the **background paper** entitled **"**Towards a trustworthy digital economy";
- undertaking **engagement activities** in relation to external stakeholders.

There are currently no plans to solicit assistance from the GPA Reference panel as part of the external engagement activities, yet this may change once the GPA Reference Panel has been established and becomes operational.

Conclusion

In the first year of its existence, PSWG2 has delivered its planned actions for 2019-20, including both deliverables as set out in its methodology and workplan. With the support of the 2020 Closed session, PSWG2 plans to engage closely with relevant multilateral and international bodies in order to give the GPA a stronger voice in global debate and initiatives surrounding the digital economy.

Annex

Towards a trustworthy digital economy

Background paper

Global Privacy Assembly

Executive summary

The digital economy represents a profound transformation of the way businesses, governments and individuals interact. A steadily growing number of transactions are now digital, powered by technologies and services that foster efficiency and innovation. The increase in data, connectivity and processing capabilities has given rise to new business models and new methods of service delivery.

While the digital economy contributes to economic growth, such growth is only sustainable if sufficient safeguards are in place to ensure trust. Without appropriate safeguards, the use of data generated by and about individuals can have significant adverse effects on their fundamental rights and interests. A lack of transparency and control, discrimination, manipulation, or unwanted disclosures of personal data are real risks that can significantly undermine trust in the digital economy. If individuals do not have sufficient confidence that their use of devices and services will not be detrimental to them, the digital economy will fail to reach its full potential.

Privacy and data protection regulations contain a variety of safeguards that help to support trust in the digital economy. Such safeguards create a framework for fair and ethical use of personal data, promote data protection by design and by default, while at the same time empowering individuals. Privacy and data protection regulations also enhance security, accountability and oversight. Each of these safeguards helps to promote a sustainable and level playing field, enhance consumer choice and prevent harms, create a competitive advantage for businesses, and act as a driver for innovation.

Background

The Global Privacy Assembly (GPA), originally named as the International Conference of Data Protection and Privacy Commissioners (ICDPPC), is the premier global forum for data protection and privacy authorities.

One of the strategic priorities of the GPA, 'Advancing Global Privacy in a Digital Age', is to work towards a global regulatory environment with clear and consistently high standards of data protection.

The current background paper serves as a basis to develop a longer-term and more coherent approach to issues around the data protection aspects of regulation of the digital economy, including through closer engagement with relevant multilateral and international bodies.

1. Introduction and scope

The digital economy represents a profound transformation of the way businesses, governments and individuals interact. A steadily growing number of transactions are now digital, powered by technologies and services that foster both efficiency and innovation. Digital transformation provides many benefits. At the same time, it also entails a series of risks. Without appropriate safeguards, the use of data generated by and about individuals can have significant adverse effects, which can undermine trust in the digital economy.

An important characteristic of the digital economy is its global nature. Worldwide ICT networks enable businesses to offer digitalised services across the globe at relatively limited start-up costs. Even small players can operate on a global scale, without any physical presence beyond their country of origin. A second important characteristic of the digital economy is the increasingly central role of a limited number of private actors who are able to shape the digital economy in ways previously reserved to public authorities.

Policymakers play a key role in the success of the digital economy, as they act as both drivers of digital innovation and guardians of public and societal interests. The main challenge for policymakers is to define and implement policies and regulatory frameworks that promote efficiency and innovation, whilst at the same time supporting security and trust.

This background paper explains how data protection and privacy regulation provides safeguards for the public and supports trust in the digital economy, without stifling responsible innovation.

The COVID-19 pandemic has elevated the importance of the digital economy, as well as the need for data protection and privacy. Communication networks, data and devices are being employed at large scale as part of efforts to manage the crisis. Measures of confinement and social distancing have greatly accelerated the pace of digital transformation. More than ever, the economy and society rely on digital approaches to daily activities, ranging from home working to home schooling. Public health management and research also increasingly relies on data and technology (e.g., contact-tracing applications for epidemiological surveillance and monitoring, AI-supported research into treatments). The extended use of digital tools can serve to further foster innovation but also increase the potential risks for data protection and privacy, cybersecurity and human rights.

Policies concerning the digital economy are developed at both national and international level. While the importance of data protection and privacy is increasingly recognised, it is rarely the focus of the policy development process. This paper serves as a primer for policymakers who wish to **promote the development of the digital economy in a coherent, fair and sustainable manner**.

To demonstrate why data protection and privacy regulation are essential for the digital economy, the remainder of this paper considers the following questions:

- What is the digital economy?
- What are important developments and trends in the digital economy?
- Why are privacy and data protection important in this context?
- How does data protection and privacy regulation benefit individuals, businesses, governments and society as a whole?

2. What is the digital economy?

Digital technologies and services have transformed economies across the globe. At the heart of the **digital transformation** are not only new technologies, but also new business models and services that rely heavily on the processing of data. The lives of citizens, the way we work and communicate has been transformed, as digital technologies become more integrated across all sectors of the economy and society.

The digital economy comprises a **wide array of activities**, ranging from traditional e-commerce (selling goods or offering services online) to digitally deliverable services (such as music streaming services, online newspapers, social media, as well as digital banking and insurance services). The digital economy also offers several innovative tools that can be used by governments in providing for the general welfare of their people, to inform policymaking and to deliver better public services to the people (e.g., e-Government public services).[i]

The digital economy is by no means limited to one particular sector of activity. Due to increasing digitalisation across sectors, the digital economy is becoming **inseparable from the functioning of the economy as a whole**.[ii] In fact, rather seeing the 'digital economy' as an optional add-on to conventional business, it should be recognised as a gradual but profound transformation of existing processes, while at the same time completely new processes emerge.[iii]

It is important to note that not all actors involved in the digital economy are consumer facing, i.e. **business-to-consumer (B2C)**. There are many **business-to-business (B2B) and business-to-government (B2G)** service providers that offer key components of the digital economy, such as IT infrastructure services (data storage, cloud computing, data analytics, high-performance computing), software solutions and AI-based digital platforms in sectors ranging from logistics, manufacturing and energy supply to mobility and public transport, environmental protection, healthcare and education. The **globalisation** of economy with supply chains interconnected over continents is greatly facilitated by the highly digitalised value chains within these sectors. The following section outlines several developments and trends to further clarify a number of important dynamics within the digital economy.

3. Developments and trends

3.1 Off-line has become on-line

Advances in network and communication technologies allow businesses to collect and exchange information in ways previously unimaginable. Computing hardware, combined with smart networks and the Internet of Things (IoT) have enabled new digitalised services to emerge that are revolutionising markets. Many consumer devices contain sensors and wireless technologies (e.g., RFID, Bluetooth, NFC) that can seamlessly capture and exchange data, effectively **blurring the boundaries** between the online and offline environment.

Box 1: Consumer wearables[iv]

Wearable technologies ("wearables") such as fitness trackers and smart watches have become commonplace. Such wearables collect data about individuals and their condition, activities and day-to-day choices. Many features of wearables are an extension of the current capabilities of smart *phones. At the same time, there are many types of sensors with different capabilities. For example, sensors have the ability to collect, in real time, information about:*

- the user's body: mood, habits, physical activities, health status, speed, mobility and

- the user's environment: images, sounds, temperature, humidity, location, social environment as well as computer-generated data to mediate the user's experience of the world around them.

3.2 From analytics to intelligence

As more connectivity leads to more digital traces, the volume of data generated on a daily basis has grown significantly.[v] A range of additional technologies and services have emerged to enable businesses to process these data efficiently at scale and to obtain additional insights which can in turn provide actionable intelligence. **Cloud computing** can be described as an "on demand" service model for IT provisioning, which typically allows customers to dynamically expand or decrease their consumption of computing resources. Due to higher internet speeds and decreased storage costs, businesses of all sizes can remotely leverage software applications and increased processing capabilities on a "pay as you go" basis.

Big data analytics refers to a set of techniques and tools used to process and interpret large volumes of data from different sources, which can be used to infer relationships, establish dependencies, and perform predictions of outcomes and behaviours. Businesses rely on big data analytics to help inform real-time decision making by combining a wide range of information from different sources.[vi]

High performance computing (HPC), also known as "supercomputing", refers to data center hardware infrastructures made of thousands of processors working in parallel to analyse billions of pieces of data in real time, performing calculations thousands of times faster than a normal computer. This aggregation of computing power delivers much higher performance than one could get out of a standard data centre in order to solve large interdisciplinary problems in science, engineering and business.

While there is no fixed definition of **Artificial Intelligence** (AI), it often refers to systems that, given a complex goal, are able to make predictions, recommendations or decisions with a certain degree of autonomy. AI systems are able to perform these functions by analysing and interpreting acquired data, processing the information derived from this data and then possibly recommending or taking the best action(s) to achieve a given goal. AI systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, speech and face recognition systems) or Internet of Things (IoT) applications with embedded AI software systems in hardware devices (e.g. autonomous cars or computer vision enabled drones).[vii]

Box 2: Smart Speakers and Virtual Voice Assistants[viii]

A smart speaker is a speaker with a built-in microphone that allows users to interact with other smart devices or internet services using their voice. The "brain" that makes the smart speaker smart is the virtual assistant. A virtual voice assistant is an interactive device made of a hardware and a software application that takes the voice of the user as its input, identifies a command or question, interacts when necessary with other services and provides a spoken response. The current generation of smart speakers typically have built-in functionalities to search for information on the internet, play music, make phone calls and manage lists. They may also allow for new functionalities and extensions, such as controlling a smart door lock, by installing third-party developed software.

3.3 New business models

The continuous increase in data, connectivity and data processing capabilities has given rise to new business models and new methods of service delivery. The offering of traditional goods and services (e.g., bike or car rental) now also takes place through mobile applications and location-based services. Varieties of digital platforms have emerged to mediate between service providers and service consumers, in virtual marketplaces consisting of professional businesses, private individuals, public actors and private organisations.[ix]

Box 3: Digital platforms[x]

Digital platforms assume a central role in digital economy. Due to network effects and the continuous expansion of service offerings, platforms are often the default go-to point for consumers and businesses alike. Digital platforms can bring together different sides of a multi-sided market and/or provide the environment to support the development and offering of new applications and services. Social media platforms, for example, now have the ability to connect users, content providers, advertisers, app developers and other companies within the same digital ecosystem.

Certain platforms have become so popular that they can exert significant and lasting market power or act as "**gatekeepers**" for businesses or public administrations seeking to reach a wide audience of potential customers or citizens. Platform providers have a major advantage in the digital economy in that they are able to record and extract insights from a growing number of transactions and other activities that takes place through their platform.[xi] Similar dynamics may occur regardless of whether the relevant markets comprise business-to-consumer (B2C), business-to-business (B2B), business-to-government (B2G) and/or consumer-to-consumer (C2C) interactions.

3.4 Personalisation

A key aspect of many modern digital services is the increasing level of personalisation that has become possible due to the significant amounts of data that individuals generate as they take part in the digital economy. This data is provided both consciously (e.g., by filling in an online form) and unconsciously (e.g., by monitoring an individual's use of a service). Using profiling techniques, such data can yield insights into individuals' preferences or interests, leading to new levels of personalisation providing each individual with a service that is specifically tailored to their preferences and characteristics. Examples include personalised results displayed by search engines, personalised music playlists, customised online banking and personalised medicine.

Whilst personalisation may have previously been a feature that could be turned on and off, it is quickly becoming a prevalent feature of many online services. As personalisation is increasingly present in many online services, policymakers should consider what controls should be available to ensure individuals are able to exercise control over the use of their personal information.

3.5 Targeting

The data generated as a result of individuals' online and offline activities are increasingly used beyond the context in which they were initially created. Location data, social media engagement and browsing behaviour across devices and services are increasingly leveraged to analyse individuals' behaviour and to infer personal characteristics in order to enable targeting of individuals for commercial or other purposes.[xii] Businesses and other actors now have the ability to target individuals with specific messages based on their actual or perceived attributes, with increased granularity, a practice often referred to as "micro-targeting".

Box 4: Micro-targeting and real-time bidding

Micro-targeting is a form of online targeted advertising that analyses personal data to identify the interests of a specific audience or individual in order to influence their actions. Micro-targeting may also be used to offer a personalised message to an individual or audience using an online service such as social media. Micro-targeting often works through the use of tracking technologies such as 'cookies', 'social plugins' and 'pixels'. These electronic tools typically track individuals' browsing habits, likes and social interactions across the internet.[xiii]

Real-Time Bidding (RTB) is a set of technologies and practices used in programmatic advertising. It has evolved and grown rapidly in recent years, allowing advertisers to compete for available digital advertising space in milliseconds, potentially involving criteria relating to politics, religion, ethnic groups, mental health and physical health.[xiv]

4. Why data protection and privacy matter

While the digital economy contributes to economic growth, such growth is only sustainable if there are sufficient safeguards in place to ensure trust in the digital economy. Unexpected or unauthorised uses of personal data can have significant adverse impacts for individuals, not just in relation to the right to privacy but also in relation to other fundamental rights and interests. This section outlines possible risks presented by the digital economy from the perspective of individuals, as well as the safeguards provided by data protection and privacy law that help promote and maintain trustworthiness.

4.1 Risks

A. Lack of transparency and control

The proliferation of connected devices and tracking technologies means that individuals' otherwise private activities are constantly being recorded. Digital techniques, such as profiling and AI, can be used to infer information about individuals that they did not actively disclose, possibly without their knowledge. Such inferences can potentially be used to influence decisions about education, job opportunities, credit decisions, insurance or price offering for example.

Box 5: Use of AI as part of the recruitment processes

To help screen among large numbers of potential job applicants, employers increasingly rely on digital technologies. Video interview platforms on the market claim to use AI to evaluate the job seeker's facial expression and how they answer during interviews in order to recommend which applicants should be given further consideration.

The lack of transparency regarding the role of the different actors involved in the digital economy complicates the ability for individuals to exercise control. This lack of control extends to individuals who are in close contact or direct interaction with the main user. Since devices and tracking technologies may have access to messages, contacts, locations or photo galleries of the main user, the personal data of non-users may also be subject to processing.

The emergence of an intricate system of private data markets involving technology companies, analytics providers and data brokers has rendered individuals increasingly transparent, while the underlying processes have become increasingly opaque. Due to the increasing complexity of systems used to deliver services within the digital economy, individuals do not always receive meaningful information that will help them to make informed decisions.

The growing information asymmetry between companies using these services and the individuals affected by them places those individuals in an increasingly vulnerable position. Unless individuals receive appropriate information and controls (e.g. in relation to the lifecycle of the data or the third parties to whom the data are disclosed), they could increasingly be subject to decisions that they do not understand or are unable to challenge. Moreover, their increased dependency towards certain platforms or an excessive targeting of offers by certain actors could reduce their possibilities of choice in the digital economy.

B. Data breaches

The personal data collected by service providers in the digital economy are an attractive target for cybercriminals and other malicious actors. Not a day goes by without reports of a security breach leading to the unintended disclosure of personal data. Such disclosures can have a range of significant adverse effects on individuals, such as identity theft or fraud, financial loss, damage to reputation or embarrassment. Loss of availability or integrity of personal data may also undermine individuals' confidence in the use of digital products and services. The more often data breaches are seen to occur, the less inclined individuals may be to share personal data.[xv]

C. Manipulation

Online advertising and targeting are, by definition, used in order to influence the behavior and choices of individuals, whether it be in terms of their purchasing decisions as consumers or in terms of their political decisions as citizens engaged in civic life.[xvi] Certain targeting approaches may however go so far as to undermine individual autonomy and freedom, e.g. by delivering individualized messages designed to exploit or even accentuate certain vulnerabilities, personal values or concerns. Observed or inferred information can be used to target the individual with specific messages and at specific moments to which he or she is expected to be more receptive, thereby surreptitiously influencing his or her thought process, emotions and behaviour.[xvii]

Box 6: Micro-targeting in the context of elections

Political campaigning intends to influence voters' behaviour via messages that are generally appealing to the intended audience. Using micro-targeting, however, political parties and campaigns to target individual voters with tailored messages, specific to the particular needs, interests and values, or to play on the fears or prejudices of specific groups. Such targeting might even involve disinformation or messages that individuals find particularly distressing, and are therefore (more) likely to stimulate a certain emotion or reaction by them. When polarising or untruthful (disinformation) messages are targeted at specific individuals, with no or limited contextualisation or exposure to other viewpoints, the use of targeting mechanisms can have the effect of undermining the democratic electoral processes.

D. Discrimination

While the predictive capabilities of data analytics may result in greater efficiencies, they may also have disparate impacts. For example, by limiting exposure to certain information, for instance in job advertisements, based on a person's gender or inferred health status, they may further perpetuate discriminatory attitudes and practices.[xviii] The potential for discrimination in advertising arises from the ability for advertisers to leverage the extensive quantity and variety of personal data (e.g. demographics, behavioural data and interests) gathered by platforms, data brokers and other actors.

Data-driven decision-making can lead to discrimination in several ways. For example, the variables used to determine a course of action may indirectly have a greater impact on certain ethnic or minority groups. It is also possible that the data used to "train" machine learning or artificial intelligences is in itself biased (e.g., through over- or under-representation of certain groups). Similarly, certain data or attributes may effectively serve as "proxies" that correlate to otherwise protected characteristics (e.g., race, gender or sexual orientation).[xix] Each of these forms of discrimination may have both tangible and non-tangible adverse effects. Discrimination may also be indirect due to the complexity of the systems and processes used, particularly with regards to AI, resulting in biases which were not immediately apparent prior to deployment.

E. Loss of trust

If individuals do not have sufficient confidence that their use of devices and services will not be detrimental to them, it may have a chilling effect on their behaviour, impacting for example the content they choose to access online or the products consumed. For example, if sensitive data collected via wearables or other connected devices is disclosed or used unexpectedly, it may hamper growth in an otherwise promising new market.[xx] Once the benefits of using a digital service no longer outweigh the risks and potential damages, individuals will be less likely to use it. The loss of trust may also adversely affect competition, as individuals may be less likely to sign up for competing services if they already have little or no trust in existing ones.[xxi] Trust is therefore absolutely key to the development of the digital economy. Fortunately, privacy and data protection regulations contain a variety of safeguards that help to support trust in the digital economy.

4.2 Safeguards

A. A framework for fair and ethical use

Data protection and privacy regulations consist mainly of technology-neutral and principle-based requirements. While those requirements determine the boundaries of (un)acceptable uses of personal data, they seldom take the form of direct prohibitions. Instead, they provide a series of rights for individuals and impose good data management practices on the part of the entities that process personal data ('data controllers').[xxii] The aim of the requirements is to prevent personal data from being processed in ways that undermine the rights and freedoms of individuals. Direct prohibitions are only imposed where the risks are particularly high (e.g., processing of special categories of data), subject to exceptions to ensure such data can still be processed for legitimate aims. As a result, data protection and privacy regulations are sufficiently flexible and scalable to support responsible innovation. Using a risk-based approach, rooted in the respect for human dignity and autonomy, data protection and privacy regulations stimulate an appropriate balance of the interests at stake.

Box 7: Key principles

While certain differences continue to exist in national and international frameworks for data protection and privacy, there is almost universal acceptance of a number of key principles and rights. Further elements, while not attracting universal agreement, reflect a relatively broad acceptance of increasingly important privacy protections in today's global environment. Such key principles include, but are not limited to:

Fairness *- The processing of personal data should not result in unlawful or arbitrary discrimination. Any processing of personal data should be within individuals' reasonable expectations and should be justifiable. Individuals should not be misled about any aspect of the processing of their personal data.*

Lawfulness *– The processing of personal data must not be unlawful and should respect any applicable national legislation. Where appropriate to the jurisdiction, processing of personal data should have a specific basis in law. In particular, where consent is an appropriate basis for legitimising processing, it should be freely given, specific, fully informed and unambiguous.*

Purpose specification *– Those organisations or individuals processing personal data should specify the purposes for the processing. The processing of personal data should be limited to fulfilling the specified, explicit and legitimate purposes.*

Proportionality *– The processing of personal data should be limited to that which is adequate, relevant and necessary in relation to the specified purpose. Processing should be limited to the minimum necessary to fulfil that purpose.*

Data quality *– Personal data processed should be accurate, complete and up to date to the extent required for the purpose.*

Data retention *– Data should be retained for the minimum necessary period in relation to the purpose. When data is no longer necessary for the legitimate stated purpose it should be deleted or rendered anonymous.*

B. Data protection by design and by default

It is unreasonable to expect individuals to conduct a detailed investigation into each company's data practices before deciding whether to use a digital product or service. As the technological complexity of the digital economy increases, individuals simply have neither the time nor the expertise to do so. Data protection by design and by default means that service providers in the digital economy need to have data protection designed into and as a default setting in the processing of personal data. It requires companies to implement appropriate technical and organisational measures and necessary safeguards to implement data protection principles in an effective manner and to protect the rights and freedoms of data subjects. Of course, the implementation of data protection by design and by default does not absolve companies from their obligation to be open, transparent and accountable (e.g., by actively informing data subjects of intended data uses and giving them the ability to obtain additional information).

If data protection by design and by default are effectively implemented, individuals can trust that their use of digital products and services will not unduly interfere with their rights and freedoms. Especially entrepreneurial young innovation-driven companies, technology start-ups and spinoff companies from public research should take no other approach than privacy by design and by default when creating, testing implementing and scaling up innovative data driven products or services.

Box 8: Optimising delivery service in a pseudonymous manner[xxiii]

Imagine a courier service that wants to assess the effectiveness of its deliveries in terms of delivery times, workload scheduling and fuel consumption. In order to reach this goal, the courier has to process a number of personal data relating to both employees (drivers) and customers (addresses, items to be delivered, etc.). This processing operation entails risks of both monitoring employees (which requires specific legal safeguards), as well as tracking customers' habits through the knowledge of the delivered items over time. These risks can be significantly reduced with appropriate pseudonymization of employees and customers. In particular if pseudonymization keys are frequently rotated and macro areas are considered instead of detailed addresses, an effective data minimization is pursued, and the controller can solely focus on the delivery process and on the purpose of resource optimization, without crossing the threshold of monitoring individuals' (customers' or employees') behaviours.

Certain privacy and data protection challenges are the result of decisions made during the product or software development phase. Manufacturers, producers and designers should therefore be encouraged to take privacy and data protection into account when developing or designing products, services and applications that are based on the processing of personal data (e.g., smart consumer objects).

C. Empowering individuals

Data protection and privacy regulations provide individuals with a series of rights to empower individuals with respect to what happens with their personal data. Companies who process personal data must be open and transparent about their processing activities and provide meaningful information in a clear and concise manner. In addition, individuals in principle have the right to access their personal data and obtain basic information about why it is processed, where it comes from and to whom it has been disclosed. If the data is no longer accurate or no longer necessary, rectification or deletion is appropriate. In addition to empowering individuals, certain rights (e.g., data portability) can also foster the development of new services and competition by facilitating switching between service providers.

D. Security

Data protection and privacy regulations require companies processing personal data to implement appropriate technical and organisational measures to ensure security. By implementing such measures, the risk of data breaches can be reduced significantly. A key element of any data security policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner.[xxiv] The security requirements contained in data protection and privacy regulations are not overly burdensome or prescriptive, instead they enable companies to bring into considerations all relevant elements, such as the state of the art, the costs of implementation and the possible risks presented by the processing.

Box 9: Data breach notification

Different data breaches may present different risks of varying likelihood. If a breach is clearly unlikely to result in a risk to the rights and freedoms of natural persons, notification to individuals or supervisory authorities would be of limited added value. In such cases, it may be sufficient for the company to take note of the breach internally and decide which remedial measures (e.g., additional staff training, software update, change in security policy) will reduce the risk of re-occurrence. Where *the breach is likely to result in a high risk to the rights and freedoms of natural persons, however, the individuals affected should be informed in clear and plain language of the nature of the personal data breach and its likely consequences. Where appropriate, companies should provide information on the measures taken or proposed to be taken to mitigate its possible adverse effects. If supervisory authorities can verify whether companies have correctly assessed the nature of the breach, individuals can have greater confidence that breaches which present significant risks will be directly communicated to them.*

D. Accountability

Accountability means that companies are not only responsible for complying with data protection and privacy regulations, but must also be able to demonstrate compliance in practice. Data protection and privacy regulation have come to introduce a variety of mechanisms designed to promote the accountability. Examples include requirements to put in place internal policies and procedures dedicated to ensure compliance, designating a data protection officer (DPO), maintaining appropriate records of processing activities, and data protection impact assessment obligations. Again, each of these measures should be tailored to the nature, scope, context and purposes of the processing, as well as the risks presented by the processing.

Accountability as a principle also facilitates a proactive behaviour from stakeholders involved in the data processing, instead of staying reactive. Data protection and privacy regulations also contain voluntary tools for conformity assessment such as certification, codes of conducts, Binding Corporate Rules. The right combination of voluntary and mandatory accountability mechanisms can really stimulate data controllers to think, plan and act ahead.

Box 10: Data Protection impact assessments[xxv]

A data protection impact assessment ("DPIA") is a process designed to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of data protection and privacy regulations, but also to demonstrate that appropriate measures have been taken to ensure compliance.

E. Oversight and redress

A trustworthy digital economy requires appropriate oversight and redress mechanisms. While individual empowerment is necessary, it is not sufficient. In light of the increased complexity of digital products and services, independent privacy and data protection authorities as well as independent courts and tribunals are necessary to ensure that data processing practices can be audited and to ensure corrective action where appropriate. The public needs some form of assurance that there are regulators ready to assist and provide them guidance for their concerns.

As individuals often do not have the resources to litigate to protect their rights, the ability to submit complaints and report possible violations of data protection and privacy regulation is of paramount importance. Awareness raising and providing accessible information is key in this respect, as individuals may otherwise not be aware of how the processing of their data affects them, either because of lack of access to information or due to lack of technical knowledge.

Independent oversight enhances trustworthiness and benefits businesses (by protecting them against competitors applying unfair practices) and governments and society as a whole, by providing (early) information about developments that put individuals' rights and freedoms at risk. Monitoring of business practices contributes to the improvement of policies not only within business organisations but can also improve the evidence base for policy-making.

Of course, all actions (and/or inactions) by a privacy and data protection authority must be subject to independent judicial review of a court or tribunal.

As personal data processing is increasingly a core part of business models in the digital economy, privacy and data protection authorities should cooperate with other appropriate bodies (e.g. consumer protection or competition oversight bodies) that can further the goal of protecting the rights of the individual in relation to their personal data and help to promote ethical, lawful and fair business practices.[xxvi]

5. Systemic benefits of data protection and privacy regulation

A. A sustainable and level playing field

Sustainable development requires models for long-term value creation that keep the needs and interests of the society, the economy and the natural environment in balance. As a result, respect for societal values and human dignity is indispensable.[xxvii] Trust is hard to gain but easily lost. While certain uses of personal data may yield economic growth in the short term, uses that are detrimental to individuals eventually become detrimental to the digital economy as a whole. Appropriate laws and regulations, combined with appropriate oversight by supervisory authorities and independent courts help to ensure that all controllers operate on a level playing field and innovate in ways that maintain consumer confidence and citizens' trust.

B. Enhancing consumer choice and preventing harms

Appropriate data protection and privacy regulation enhance the ability of consumers to receive services on the terms they prefer and to make choices about the services they seek in accordance with their own values. It also reduces consumer harm by addressing practices which have negative effects and about which consumers cannot make choices, either because of deception, lack of transparency, or fraud.

C. A competitive advantage

Given the importance of trust in the digital economy, companies with a reputation of taking data protection and privacy seriously have a clear advantage over their competitors. With consumers becoming increasingly aware of the risks of data misuse, data protection and privacy have become a real selling point. Indeed, having a strong reputation in privacy and security can serve to attract more customers. Rather than being a regulatory burden, good privacy and data protection practices signal to consumers and citizens that their personal data will be treated with respect, which will increase their confidence.[xxviii] Good privacy and data protection practices also offer new opportunities to facilitate international data flows, between commercial operators or public authorities.[xxix] As a result, having good privacy safeguards in place is in the interest of the individuals, business and governments concerned.

D. A driver for innovation

Data protection and privacy regulations not only promote responsible innovation, they themselves also act as drivers for innovation. For example, new types of intermediaries and economic operators have emerged that provide services that make it easier for individuals to control and share their personal data. So-called personal information management systems ("PIMS") seek to transform the current provider-centric system into a human-centric system whereby individuals are given increased transparency as well as user-friendly tools to participate in the use and distribution of their personal data. Such increased transparency, accompanied by adequate legal and technical safeguards ultimately promotes greater consumer confidence and trust.[xxx] One can also see an increase in economic operators seeking to offer privacy-friendly alternatives to existing digital services, for example in the area of online advertising.

Box 11: Contextual vs. behavioural advertising

Contextual advertising is a form of targeted advertising for advertisements appearing on websites or other media, whereby the advertisements are selected and served based on the context of what a user is looking at. The main difference with online behavioural advertising methods is that advertisements are tailored to the content near which they are displayed, rather than the profile of the individual viewing the content. In addition to having the potential of being more privacy-friendly, certain media websites have already reported increased conversion rates since moving away from behavioural advertising based on profiling and real-time bidding and other forms of micro-targeting.[xxxi]

An increasing number of data protection and privacy regulators also seek to support responsible innovation through "regulatory sandboxes" or "testbeds" to help companies who are developing products and services that use personal data in innovative and safe ways. Such approaches help companies deliver new products and services of real benefit to the public, with assurance that they have tackled built-in data protection at the outset.[xxxii] At the same time, it allows authorities to keep pace with new and emerging digital opportunities.

6. Conclusion: providing safeguards for the public and supporting trust

A vibrant digital economy consists of products and services that respect the rights and interests of individuals. If used effectively, data can become an enabler for a better society, e.g. through improvements in health and well-being, environment, transparent governance and convenient public service. Laws and regulations are necessary safeguards, however, to counter theft of personal data, to set rules for how personal data can be collected and used, and to ensure that data-driven business models generate gains for society as a whole[xxxiii] and are therefore sustainable in the long run. Policymakers and business who think long-term will realise that data protection and privacy regulations are indispensable for a trustworthy digital economy.

Policymakers should therefore consider data protection and privacy regulations as essential building blocks to promote responsible and sustainable innovation. By empowering individuals with a number of basic rights and protections, individuals will be able to more confidently enjoy the benefits that the digital economy has to offer. Supervisory authorities with the resources and technical expertise necessary to exercise their powers effectively and to make impartial decisions ensure that companies operate on a level playing field. But policymakers should not stop there. Complementary measures, including education and awareness raising, skills development, and the promotion of privacy-enhancing technologies and services should be high on the agenda of any policymaker seeking to promote a fair and sustainable digital economy.

ENDNOTES:

[i] EU, “Towards a European strategy on business-to-government data sharing for the public interest”, Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64954

[ii] United Nations Conference on Trade and Development (UNCTAD), “Digital Economy Report 2019 - Value creation and capture: implications for developing countries”, 2019, p. 26, available at https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=2466.

[iii] P. Chase a.o., “Transatlantic Digital Economy and Data Protection: State-of-Play and Future Implications for the EU's External Policies”, Directorate-General for External Policies of the European Parliament”, 2016, p. 5, https://www.europarl.europa.eu/RegData/etudes/STUD/2016/535006/EXPO_STU(2016)535006_EN.pdf.

[iv] Office of the Privacy Commissioner of Canada, Wearable Computing - Challenges and opportunities for privacy protection, Report prepared by the Research Group of the Office of the Privacy Commissioner of Canada
2014, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/wc_201401/

[v] United Nations Conference on Trade and Development (UNCTAD), “Digital Economy Report 2019”, United Nations, 2019, p. 27, https://unctad.org/en/PublicationsLibrary/der2019_en.pdf.

[vi] Organisation for Economic Cooperation and Development (OECD), *OECD Digital Economy Outlook 2017*, p. 24, https://www.oecd.org/internet/oecd-digital-economy-outlook-2017-9789264276284-en.htm.

[vii] High-Level Expert Group on Artificial Intelligence, “A definition of AI: Main capabilities and scientific disciplines, April 2019, p. 8 and OECD, *OECD Digital Economy Outlook 2017,* p. 25. See also European Data Protection Supervisor (EDPS), Artificial Intelligence, Robotics, Privacy and Data Protection - Room Document for the 38th International Conference of Data Protection and Privacy Commissioners, October 2016, available at https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf

[viii] European Data Protection Supervisor, TechDispatch #1: Smart Speakers and Virtual Assistants, 19 July 2019, https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-1-smart-speakers-and-virtual_en

[ix] Organisation for Economic Cooperation and Development (OECD), Challenges to Consumer Policy in the Digital Age, Background Report G20 International Conference on Consumer Policy, 2019 p. 7-8, https://www.oecd.org/sti/consumer/challenges-to-consumer-policy-in-the-digital-age.pdf.

[x] Based on United Nations Conference on Trade and Development (UNCTAD), “Digital Economy Report 2019”, p. 25-27.

[xi] United Nations Conference on Trade and Development (UNCTAD), “Digital Economy Report 2019”, p. 16.

[xii] European Data Protection Supervisor (EDPS), Opinion 3/2018 on online manipulation and personal data, 2018, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

[xiii] Information Commissioner’s Office (ICO), “Microtargeting”, https://ico.org.uk/your-data-matters/be-data-aware/social-media-privacy-settings/microtargeting/ ; L. Ketscher a.o., “Powering the digital economy: Regulatory approaches to securing consumer privacy, trust and security”, ITU Publications, Thematic Reports - Regulatory & market environment, 2018, p. 15, https://www.itu.int/pub/D-PREF-BB.POW_ECO-2018; European Data Protection Supervisor, Opinion 3/2018, p. 7-8.

[xiv] https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf

[xv] L. Ketscher a.o., “Powering the digital economy: Regulatory approaches to securing consumer privacy, trust and security”, ITU Publications, p. 36.

[xvi] European Data Protection Supervisor, Opinion 3/2018, p. 18.

[xvii] See ‘Experimental evidence of massive-scale emotional contagion through social networks’**,** Adam D. I. Kramer, Jamie E. Guillory, and Jeffrey T. Hancock, PNAS June 17, 2014 111 (24) 8788-8790; first published June 2, 2014 https://doi.org/10.1073/pnas.1320040111, available at: https://www.pnas.org/content/111/24/8788.

[xviii] European Data Protection Supervisor, Opinion 3/2018, p. 10.

[xix] F. Zuiderveen Borgesius, “Discrimination, artificial intelligence, and algorithmic decision-making”, Study for the Anti-discrimination Department of the Council of Europe, February 2019, available at https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73.

[xx] L. Ketscher a.o., “Powering the digital economy: Regulatory approaches to securing consumer privacy, trust and security”, ITU Publications, 2018, p. 16-17.

[xxi] L. Ketscher a.o., “Powering the digital economy: Regulatory approaches to securing consumer privacy, trust and security”, ITU Publications, 2018, p. 16-17.

[xxii] De Hert, P. and Gutwirth, S. “Privacy, data protection and law enforcement. Opacity of the individual and transparency of power”, in E. Claes, A. Duff and S. Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerpen/Oxford, Intersentia, 2006, p. 76 and following.

[xxiii] European Data Protection Board (EDPB), “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default” (version for public consultation), 13 November 2019 p. 20,

https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

[xxiv] European Data Protection Board (EDPB), "Guidelines on Personal data breach notification under Regulation 2016/679", 6 February 2018, WP 250rev.01, p. 6, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

[xxv] Article 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA)", WP248rev.01, 4 October 2017, p. 4, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

[xxvi] Resolution to support and facilitate regulatory co-operation between data protection authorities and consumer protection and competition authorities to achieve clear and consistently high standards of data protection in the digital economy, 41st International Conference of Data Protection and Privacy Commissioners October 2019, Tirana, Albania available at https://edps.europa.eu/sites/edp/files/publication/dccwg-resolution_adopted_en.pdf.

[xxvii] Finland's Presidency of the Council of the European Union (EU2019.FI), "Principles for a human-centric, thriving and balanced data economy", 2019, p. 2, https://dataprinciples2019.fi.

[xxviii] L. Ketscher a.o., "Powering the digital economy: Regulatory approaches to securing consumer privacy, trust and security", ITU Publications, 2018, p. 19 and 28.

[xxix] European Commission, Communication from the Commission to the European Parliament and the Council, "Exchanging and Protecting Personal Data in a Globalised World, COM/2017/07 final, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN.

[xxx] European Data Protection Supervisor (EDPS), Opinion 9/2016 on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data", 20 October 2016, p. 5-6, https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf.

[xxxi] J. Ruiz, "Is ethical ad-tech possible?", Open Rights Group, 2020, https://www.openrightsgroup.org/blog/2020/is-ethical-ad-tech-possible

[xxxii] Information Commissioner's Office (ICO), "The Guide to the Sandbox (beta phase)", 2019, https://ico.org.uk/for-organisations/the-guide-to-the-sandbox-beta-phase/

[xxxiii] United Nations Conference on Trade and Development (UNCTAD), "Digital Economy Report 2019", p. 20.