Business at OECD Guiding Principles for the Review of the 2013 OECD Privacy Guidelines

November 2019
Introduction

Digitalization offers unprecedented opportunities to raise efficiency and productivity, enable creativity and innovation, and increase competition and consumer welfare, while fostering social and economic progress.

While there will be challenges, recent studies suggest that the potential benefits of digitalization will prevail. The expected economic impact of digital technologies is underlined by estimates\(^1\) that the Internet of Things (IoT) will add between $2.7 trillion and $6.2 trillion to the global economy annually by 2025. According to PwC’s Global Artificial Intelligence (AI) Study, AI could contribute up to $15.7 trillion to the global economy by 2030 – due to increased productivity and consumption side effects.

Data flows in and out of the United States alone are estimated at 80 terabytes per minute—eight times the size of the entire print content of the Library of Congress. Since 2005, they have increased by a factor of 80, from just 5 terabits per second to an estimated 400 per second. By 2020, consumers are expected to spend $1 trillion on cross-border e-commerce. These flows are more than just consumer transactions and social media posts. They are an integral part of the way companies now operate. According to McKinsey Global Institute (MGI), cross-border data flows already make a larger contribution to global GDP than the goods trade.\(^2\)

Business has a key role to play in ensuring that economies harness the greatest benefits from digital enhancements to the means of doing business, making our economies more efficient and productive, while maintaining safety, security and privacy of data.

The importance of Trust

There is a need to build greater public trust in the digital economy by ensuring the privacy of personal data. The benefits of technology innovation enabled by data flows and responsible data use will only be realized and embraced by consumers, businesses, and governments who trust the online environment and feel confident that the privacy of their personal data will be respected. Compliance with privacy regulations and the responsibility to adopt recognized best practices is a top priority for business to ensure that personal data and information is appropriately secured as technology and services evolve.

Strong Privacy Laws are needed with reasonable interpretation and application

Strong privacy laws are those that promote transparency, individual empowerment (particularly through data subject rights), corporate accountability (particularly through privacy by design, including data protection impact assessments) and strong enforcement across all sectors. Privacy laws should also build in appropriate flexibility to ensure that innovative uses of data may take place when subject to the proper safeguards.

Such laws are necessary for a healthy, innovative digital economy. People won't fully engage with digital services unless they trust that their privacy is protected and their data secured. The key will be promoting reasonable interpretation and application of laws and interoperability of global laws. The OECD should encourage the further development of strong privacy laws that are interoperable, which will build a foundation for data flows with trust.

---

Privacy-protective data flows enable innovation and maximize economic opportunities between countries that adopt complementary frameworks. The discussions underway in the Asia Pacific Economic Cooperation (APEC) forum with the European Commission aimed at mapping common elements of the APEC Cross-Border Privacy Rules (CBPR) system and the GDPR serves as a good example as does Japan’s Data Free Flow with Trust (DFFT) initiative.

**Business at OECD priorities for the review of the 2013 OECD Privacy Guidelines: Guiding Principles**

In 2019 the OECD is working with countries and experts to scope developments and provide practical recommendations on the implementation of the Guidelines in today's digital environment. Ensuring a healthy, innovative digital economy, while also ensuring privacy protections that build trust is essential. *Business at OECD* advocates the following guiding principles in undertaking this review.

- **The Globally Recognized Guidelines for Privacy**

  The OECD’s 2013 Privacy Guidelines must remain the global “standard”\(^3\) for privacy policy principles. The OECD’s five-year review, being undertaken in 2019, should focus on refinements that ensure its continued longevity. The OECD should not “regulate against change,” but pursue a measured approach that can be adapted to the privacy implications of technology innovations.

- **Accountability**

  Business and government must be responsible for the privacy of data throughout its life cycle. Transparency and individual participation, including through user consent, remain key principles for processing personal data. But consent is not always appropriate or desirable, and other legal grounds must be available, as they are in frameworks such as the GDPR. For instance, requiring individuals’ consent to process their personal data for fraud prevention purposes is not meaningful as perpetrators of the fraud would refuse consent; more importantly the stability and integrity of the payment ecosystem cannot be made dependent on individuals’ choices.

  Even where individuals’ consent is obtained, consent alone is not sufficient. Companies should be responsible for ensuring that consumers are protected throughout the online experience. Accountability measures should include the designation of a data protection officer and the regular performance of documented impact assessments for activities creating high risks for individuals’ privacy, which can be reviewed upon request by relevant government authorities.

  Identified impacts of data processing on the rights and freedoms of individuals should be mitigated through documented safeguards, such that the benefits of processing personal data outweigh the residual risks. Such accountability measures are consistent with the OECD Guidelines for Multinational Enterprises and are fundamental to creating a culture of responsible data management. These measures also allow for the repurposing of data in ways that allow technological innovation and economic development without prejudicing the rights and interests of consumers.

---

\(^3\) The term “standard” is used colloquially here and not referring to technical standards.
• Enforcement

Enforcement of privacy policies is a factor in building public trust in information technologies and the digital economy. While the OECD Privacy Guidelines are widely accepted policy principles, data protection problems, such as massive personal data breaches and lack of transparency to consumers regarding sharing/use of personal data, are a challenge to building trust. An OECD review of the 2013 Privacy Guidelines should explore enforcement mechanisms and examine their relationship privacy outcomes. A review can determine common approaches and challenges to enforcement as well as explore good practice.

• Proportionality

Proportionality is critical for the implementation of accountability. Data privacy is not the sole domain of big companies. Accountability processes also need to be understood and readily implementable by SMEs. Accountability obligations should be applied to organizations on a proportional basis, taking into account the size and capabilities of an organization, as well as the amount of data and types of data-driven activities that the organization is conducting. To encourage SMEs to conduct risk assessments governments should consider a company's having conducted a good faith risk assessment as a mitigating factor when evaluating compliance.

• Transborder Data Flows

The OECD Privacy Guidelines have aimed to facilitate the cross-border flow of data since their adoption. Cross-border flows of data enable economic development, participation in global value chains, and technological innovation. Laws and policies should not unnecessarily restrict cross-border flows of data, including by mandating the local storage of data.

Instead laws should facilitate cross-border data flows that are protected through appropriate technical and legal measures. Cross-border transfer restrictions, while often well-intentioned, can be difficult to implement, damaging to the local economy, and insufficient to address the primary privacy and security concerns associated with data processing. Similarly, requiring consent as a basis for transferring data across borders also does not address the relevant privacy and security issues. Finally, data localization requirements – often developed with the intent to protect and secure data – not only serve as a barrier to data flows but also defeat the purpose of the regulations by making the data even more vulnerable to privacy and security breaches.

A more effective approach is adoption of laws that are interoperable with global technical standards or execution of standard contracts that protect personal data regardless of its location. Such an approach can help to improve resiliency and security and make data processing services more efficient by reducing latency. Companies should be responsible for making sure that the personal data they process is protected regardless of the location to which it is transferred.

To bolster accountability for cross-border data transfers, OECD Member States should continue to support and possibly strengthen mechanisms such as the Global Privacy Enforcement Network and the APEC Cooperation Arrangement for Cross-Border Privacy Enforcement, both of which promote cross-border cooperation in privacy enforcement.
• **Global Interoperability**

It is imperative that we bridge regulatory differences so there is less fragmentation, data flows seamlessly, and the digital economy continues to evolve with fair and market-based competitiveness. People deserve to know that their information will be protected wherever it travels, and a consistent global approach to privacy will help companies of all sizes comply with the law. In pursuing development of an interoperable approach, however, it is equally important to incorporate sufficient flexibility so that privacy frameworks promote consistent consumer trust in data-driven technologies around the world while enabling companies and organizations to use and transfer data in innovative ways that benefit society.

The OECD’s 2013 Privacy Guidelines were developed to ensure this balance and, in our view, serve as the model for globally accepted principles. We further note that the OECD’s 2011 Principles for Internet Policy Making, which continue to serve as the basis for building consensus on a wide range of Internet-related policy issues, expressed the general objective of OECD members to improve global interoperability of privacy frameworks through international arrangements that give practical effect to the OECD Privacy Guidelines.

Interoperability of global privacy obligations will enable compliance at scale and support trade and economic growth. Individuals and organizations should be able to use or purchase a single online service which complies with global laws and to enter global markets confidently, boosting both innovation and compliance.

• **Multistakeholder Approach**

The OECD is uniquely placed to consider and develop a globally interoperable digital privacy policy framework as it recognizes and gives weight to the input of non-governmental stakeholders alongside with government Members. Given the rapid pace of technological change, it is critical for business, the technical community, and civil society to advise governments whether elements of a privacy policy framework are commercially viable, technically feasible, and offer adequate personal privacy protections. Importantly, stakeholder inclusion can lower the risk of unintended consequences and increase legitimacy and adoption of policies and regulations.

• **Enabling Continued Innovation and Emerging Technologies**

The OECD and its member governments should carefully consider the potential impact of the 2013 Privacy Guidelines on innovation and emerging technologies including artificial intelligence, blockchain technology, big data analyses and Internet of Things, and identify areas for further clarification and multistakeholder discussion.

AI and other virtual/augmented reality technologies are in the initial stages of commercial deployment and will continue to evolve and develop. We believe that the existing Privacy Guidelines establish a necessary foundation for responsible development of these services. New requirements should be carefully considered in consultation with stakeholders to ensure they are narrowly tailored to address specific concerns. New mechanisms may also be identified in consultation with stakeholders to enable innovation and emerging technologies.
Established in 1962, Business at OECD stands for policies that enable businesses of all sizes to contribute to growth, economic development, and societal prosperity. Through Business at OECD, national businesses and employers’ federations representing over 7 million companies provide and receive expertise via our participation with the OECD and governments promoting competitive economies and better business.