
OECD Going Digital Summit - Issues Note

Session 13: A Data-Driven World - Can we Ensure Privacy?

Personal data have come to play an increasingly important role in our economies and everyday lives, and new technologies and responsible data use are yielding great societal and economic benefits. At the same time, the abundance of personal data gathered, processed and exchanged has elevated the risks to individuals' privacy.

Data-driven innovation

More and more organisations today are leveraging large volumes of (digital) data generated from myriad transactions and production and communication processes. These large streams of data, which are now commonly referred to as “big data”, are generated through information and communication technologies (ICTs) including the Internet, and increasingly, the Internet of Things (IoT) and artificial intelligence (AI). The effective use of data, in combination with data analytics (software), generates information of social and economic value. It is driving knowledge and value creation across society; fostering new products, processes and markets (referred to as “data-driven innovation” (DDI)); spurring entirely new business models; transforming most if not all sectors in OECD countries and partner economies; and thereby enhancing economic competitiveness and productivity growth.

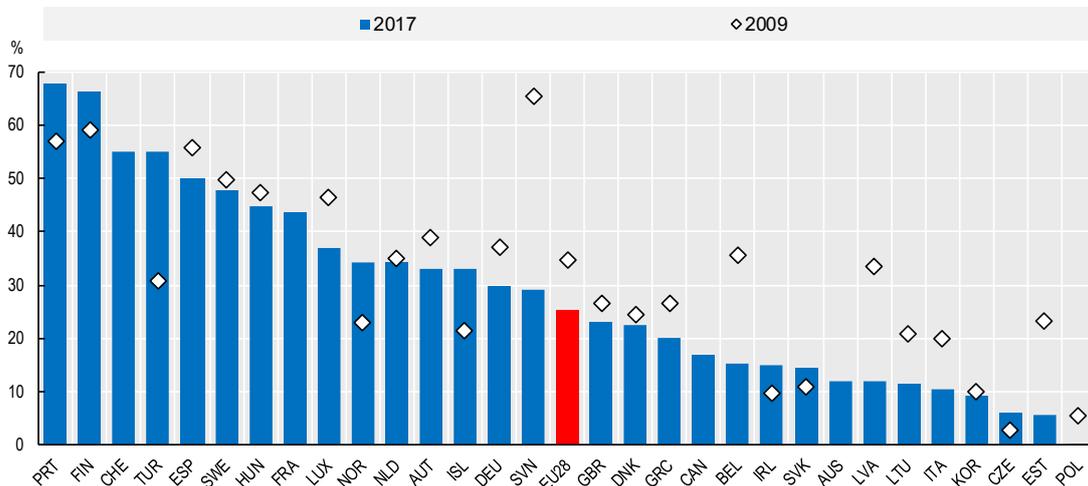
Rising privacy concerns

Critical to reaping the substantial economic benefits of DDI – as well as to realising the full social and cultural potential of that innovation – is the key element of trust. In the context of the digital economy, the main components of trust are security and privacy. As firms, Internet service providers and governments collect and store greater volumes of personal data, privacy risks increase. Personal data are being increasingly used in ways unanticipated at the time of collection, and new powerful analytics may increase the risk of disclosure of sensitive information or to link supposedly anonymous data to specific individuals. Often, this may occur without the knowledge or understanding of the individuals concerned: indeed, while privacy notices are on the rise, information asymmetries remain and users' ability to make meaningful choices regarding their privacy is lacking. Moreover, with the growth in use and value of data, personal data breaches have become more common. These risks implicate not only the individuals concerned, but the core values and principles which privacy and personal data protection seek to promote, including individual autonomy, equality and free speech, which may have a broader impact on society as a whole.

These concerns are real and remain prevalent in many countries (Figure 1). They can affect both individuals' behaviour and economic outcomes.

Figure 1. Security and privacy concerns remain prevalent in many countries

Individuals who did not buy online for payment security or privacy concerns, as a percentage of Internet users who ordered goods or services over the Internet more than a year ago or who never did, 2009, 2017



Source: OECD, based on (Eurostat[15]), *Digital Economy and Society Statistics (database)*, <http://ec.europa.eu/eurostat/web/digital-economy-and-society/data/comprehensive-database>; national sources (accessed December 2018)

Transborder data flows and regional convergence of privacy frameworks

Individuals and organisations rely more than ever on data collected, stored, processed and transferred from other entities, often located abroad. Transborder data flows are not only a condition for information and knowledge exchange, but also a vital condition for the functioning of globally distributed data markets and societies. Concerns are emerging about restrictions to transborder data flows such as data localisation requirements (including for data other than personal data), which force organisations to restrict data access, sharing and re-use within national borders. This remains an issue despite the wide recognition for the need for international arrangements and interoperability between privacy frameworks as articulated in the 2013 OECD Privacy Guidelines.

Q1: How can policy makers unlock the potential of data-driven economy without compromising privacy?

Q2: How can regulators and policymakers meaningfully cooperate to ensure interoperability of privacy frameworks globally?

Q3: More than half of privacy measures across OECD countries aim to raise awareness and empower individuals: what policy measures or initiatives have proven useful (or not) in educating and raising awareness to privacy issues?

Q4: How can the OECD help in addressing these challenges?