BUSINESS at OECD

***Business at OECD* Statement**

Unlimited Government Access to Personal Data Held by the Private Sector: *Impact on Cross-Border Data Flows and Economic Growth*

28 September 2020

Introduction

This *Business at OECD* (BIAC) statement addresses the issue of *Unlimited Government Access to Personal Data held by the Private Sector* in the context of the current review of the OECD Privacy Guidelines. We agree that unlimited government access (UGA) to personal data – specifically the interplay of UGA with cross-border data flows and data localization measures – can touch on aspects of the review of the OECD Privacy Guidelines. Work undertaken by the OECD on UGA should be narrowly focused on these aspects that are unique to the ongoing review.

Adoption of the OECD Privacy Guidelines reflects the twin aims of increasing protections for privacy and advancing the free flow of information among Member and non-member Countries. Importantly, the Guidelines have formed the basis for data protection laws in a large number of countries around the world, furthering the goal of interoperability of rules and protections.

To address the challenges of an increasingly digitally-integrated world in ways that respect governments' authority to enforce their laws and individuals' rights, it is important to strike a balance that gives individuals more control over their data, promotes digital security and rule of law, and provides the tools that governments, courts, and law enforcement need to keep their communities safe.

Issue

Unlimited government access to personal data held by the private sector, including for stated national security reasons, negatively impacts trust in the digital economy, creating uncertainty with adverse market effects. Fear of such access can cause businesses and organizations to hesitate regarding the transfer to, or storage or processing of personal data in, countries that may allow government access without appropriate safeguards, as this may jeopardize businesses' and organizations' abilities to protect their customers' privacy and to comply with applicable privacy laws. Government access requests may be for data related to individuals or to all business transactions carried out within the governments' jurisdictions.

Without clear parameters and rules around government access to personal data, including access across international borders, an atmosphere of legal uncertainty will remain, and we are likely to see governments continue to seek to address that uncertainty through data localization measures, which negatively impact cross-border data flows and the global digital economy.

Concerns and Recommendations

Businesses share a concern that government access to personal data, if not accompanied by safeguards, will negatively impact trust in the digital economy. *Business at OECD* emphasizes that unlimited government access to data can impact businesses' ability to adequately protect the privacy and security of customers' personal data, and also notes the following concerns:

- **Potential conflicts of law with third countries** – where government access to data conflicts with other legal frameworks to which a business may be subject, or where authorities at different levels (local, national, or regional) may lack sufficient coordination, there may not be robust mechanisms available to raise and seek to resolve such conflicts.

- **Lack of clarity or transparency regarding the scope of government access** – legal and business uncertainty can be created if the legal framework and safeguards applicable to government access is unknown or shrouded in secrecy. Lack of transparency may amplify distrust in government and those responsible for public safety, and decrease the legitimacy of government institutions.\

- **Data localization trends** – governments may pursue data localization measures in part to protect their companies' and consumers' data from access by third-party governments or to increase their own ability to access personal data by requiring the data be held within their borders. Such data localization policies may not measurably advance these objectives and instead negatively impact economic growth in countries pursuing such policies, as well as the global economy.[1]

- **Unlimited government access to data could create a chilling effect on individuals, discouraging their participation in the global digital economy and undermining trust in digital services.**

In considering how policymakers can create lasting rules and standards that facilitate legitimate government access, including for law enforcement, while protecting individuals' privacy, the principles of transparency, proportionality and accountability are critical to striking the right balance. *Business at OECD* recommends that the following principles be considered as part of the review of the OECD Privacy Guidelines and the promotion of trusted government access to personal data:

- The rules, laws, and international agreements that allow for government access to data should be clear as to the information, which can be accessed and the authorities empowered to access it. The legal framework should be publicly available and developed through processes that are open, transparent, and with opportunities for meaningful multistakeholder input.

- Demands for access to data should be predicated on prior independent review and approval (other than in duly substantiated cases of urgency), with such review considering the necessity and proportionality of the request and the specific evidence supporting it.

- Government access should be narrowly tailored and subject to robust independent oversight mechanisms and bodies.

- Demands on companies for access to the data that they hold should include details about such prior review, the purpose or underlying legal basis for the demand, the definition of public interest or legitimate interest in case of emergency situations, and the mechanisms available to companies or organizations to challenge the demands. Absent narrow circumstances, such as an ongoing investigation or emergency or where it might imperil public safety, individuals and organizations should be provided with notice regarding government access to their data.

- Public authorities must respect the principle of data minimization when they seek access to data. For example, in the context of the COVID-19 pandemic, governments have sought access to personal health data in order to manage public health responses. BIAC generally advocates for government access to be limited to aggregate and anonymized data, unless authorities demonstrate a significant need in the course of an independent review and approval process.

- Governments should issue public statistical reports on the exercise of their powers to access personal data from private sector entities.

[1] BIAC further notes that data localization measures increase costs for businesses, to the detriment of small and medium sized enterprises (SMEs). For consumers, data localization measures can mean fewer choices and higher prices.

- Internationally interoperable legal regimes and international agreements should advance frameworks that minimize conflicts of law and create mechanisms to resolve conflicts that do arise.

Role of OECD:

Business at OECD appreciates the OECD Secretariat's efforts to establish evidence of the impact of unlimited government access to personal data and data localization.

We recommend that the OECD Privacy Guidelines review process focuses on collecting evidence on the economic impacts of these issues, as well as best practices for trusted government access.

We would hope that these efforts can be focused on:

- The economic impact of government access and localization measures locally and globally, and the effectiveness of these measures in addressing governments' concerns regarding access to data;
- Best practices for international cooperation among governments to clearly define the rules for cross-border access to data, while ensuring high standards of privacy that protect fundamental rights; and
- Those aspects of data localization and unlimited government access to personal data that would merit additional clarification as they relate to the implementation of the OECD Privacy Guidelines.

BUSINESS at OECD

***Business at OECD* (BIAC)**
13-15 Chaussée De La Muette
75016 Paris
France
contact@biac.org | @BusinessAtOECD | www.businessatoecd.org

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.