Joint Business Statement on the OECD Committee on Digital Economy Policy's work to develop an instrument setting out high-level principles or policy guidance for trusted government access to personal data held by the private sector

5 May 2021

We commend the OECD Committee on Digital Economy Policy (CDEP) on its effort to bolster trust and minimise disruptions to global data flows with a set of high-level principles on government access to personal data held by the private sector.

OECD members share common interests in preventing, investigating, and prosecuting serious crime, as well as in addressing national security threats. OECD members also share a firm commitment to protecting the rights and freedoms of individuals, including the fundamental right to privacy, when personal data is subject to government access. When governments lose sight of these common values, conducting business can become costly and infeasible for organisations of all sizes across all sectors, especially when the cross-border free flow of data that is essential to domestic and multinational business operations and communications is restricted.

The CDEP has an opportunity to articulate principles on trusted government access to personal data held by the private sector that are common to OECD members with strong traditions of respect for human rights and the rule of law. It can offer clarity and transparency around these shared values, which will contribute to increasing trust among governments on these issues, and separately for businesses and internet users concerning the sufficiency of the protections that are guaranteed when individuals' data is being transferred to a third country or accessed by a third country's government. A more predictable environment for global data flows will enable the current pace of digital transformation to be maintained, at a time when economic recovery is top of mind for governments around the world.

As members of the business community, we strongly support this effort and look forward to 1) contributing our insights on the economic impact of the current lack of legal certainty and clarity, and 2) supporting the articulation of shared principles and important safeguards to ensure trusted government access to personal data.

We believe that the benefits of trade depend on the trusted flow of data between countries. To take just one example, the international collaborations on COVID-19 research and responses demonstrate how these flows have enabled new discoveries, information sharing, and collaboration, to help mitigate the global crisis by enabling better understanding of the virus, tracking of the spread of the pandemic and evolution of the different variants, and development and distribution of vaccines. At the same time, global data flows have enabled more efficient production, manufacturing and distribution of much needed medical equipment, along with the digital services that are foundational to the continuity of our lives, our communities, societies and governments.

Nevertheless, we are seeing trust in international data flows being eroded over concerns that government demands to access data may conflict with universal human rights and freedoms, including privacy rights, or cause concerns and conflicts with domestic laws when such access transcends borders. These increased concerns and reduced trust have led to uncertainty that may discourage individuals', businesses', and even governments' participation in a global economy, and can negatively impact economic growth.

Disruption to cross-border data flows has significant impact on business and the economy: Data transfers are estimated to contribute $2.8 trillion to global GDP—a share that exceeds the global trade in goods and is expected to grow to $11 trillion by 2025.[1] This value is shared by traditional industries like agriculture, logistics, and manufacturing, which realise 75% of the value of the data transfers.[2] With 60% of global GDP digitised by 2022, and growth in every industry driven by data flows and digital technology,[3] disruptions in cross-border data flows will have broad reverberations that can lead to reduced potential GDP gains, reduced investments in local markets, job losses and consequently welfare losses, and adverse impact on the local/national digital ecosystems – at a time when economic recovery is top of agenda for every government.

We see the following three factors as major contributors to this erosion of trust.

1. **Concerns about government access are directly impacting global data flows:**

   The lack of clarity, transparency, and consistency between national approaches to government access to data has led to a steady growth in the number and restrictiveness of measures to constrain cross-border data flows. For example, differences in approaches between the EU and the US in the protection of personal data have led to the Court of Justice of the EU's ruling in *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (Schrems II).* Some interpretations of the judgment put extraordinary pressure on organisations to restrict cross-border data flows between the EU and other countries. The European Data Protection Board's draft recommendations on additional safeguards to be adopted when using Standard Contractual Clauses (SCC) might severely limit companies' abilities to conduct cross-border data transfers, and, in some cases, to impede these transfers, with potential impact on multinational operations altogether.

[1] OECD, *Measuring the Economic Value of Data and Cross-Border Data Flows*, 297 OECD Digital Economy Papers 24 (August 2020).
[2] McKinsey Global Institute, *Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity* (May 2011).
[3] Hamilton, Daniel D., and Quinlan, Joseph P., *The Transatlantic Economy 2020* (2020), available at https://transatlanticrelations.org/publications/transatlantic-economy-2020/.

2. **Compelled data localisation requirements can be counterproductive in practice:**

   Compelled data localisation measures impact both local companies operating in a single jurisdiction (for example by preventing them from accessing global products and services, global supply chains and customers in foreign markets), and multinational companies operating in multiple jurisdictions (making it difficult, for example, to manage hiring and human resources functions from a single headquarters, to evaluate the performance of connected vehicles from a single research hub, and to analyse cybersecurity threats at different points in communications networks).

   Across all industries, technical measures are increasingly being deployed broadly to respond to compelled data localisation requirements, including safeguards to attempt to limit government access to data. These measures can in some cases impact the benefits and functionality of any globally interconnected business regardless of size. For example, they can prevent companies from offering a broad array of features that are critically important to consumers, such as cybersecurity measures, and can also prevent the analysis of data originating from multiple sources in a way that leads to global insights and remediating actions. Taken together, these factors risk undermining the economies of scale that are at the core of the digital transformation, including the enablement of micro, small and medium-sized enterprises, and the growth of innovation ecosystems domestically.

   Data mirroring mandates similarly increase the cost of doing business in a jurisdiction by requiring companies to keep a constantly updated backup of data in country.

   Ultimately, compelled data localisation mandates by governments do not resolve the existing conflicts of laws between countries that often prevent companies from responding to a foreign government's legitimate law enforcement requests. Instead, they are likely to exacerbate those conflicts, which can put businesses in an impossible position.

3. **Lack of trust has broader societal consequences:**

   Concerns over government access to personal data significantly contribute to public sectors' reluctance to avail themselves of the benefits of the digital economy, as fears grow that third-party governments will have access to data over which they previously maintained exclusive control.

For these reasons, we emphasise the **urgency of articulating common practices shared by OECD members on trusted government access to personal data held by the private sector** and believe that the OECD is in a unique position to spearhead this global effort. The CDEP can reinforce the strong traditions of OECD members in respecting the rule of law, alleviate uncertainty on these issues, and ultimately help to expand trust in trade and digital technologies. An OECD instrument setting out high-level principles and guidance, outlining necessary shared safeguards to ensure a high standard of privacy, would be a critical contribution to set a firm foundation for building trust, similar to the OECD Privacy Guidelines and its Council Recommendations on Artificial Intelligence.

We agree with CDEP's focus on safeguards—including limitations on access and use, transparency in reporting, as well as independent oversight—that are common to OECD Member States in the law enforcement and national security contexts. The OECD also has

opportunities to frame these issues within a broader digital transformation policy framework, taking a more holistic approach that would consider other relevant policy approaches and agreements.

Once that foundation is firm, we encourage like-minded governments to recognise principles identified by OECD as a basis for long-term political and legally secure mechanisms that support the continuance and development of international data flows. In addition, like-minded governments should acknowledge the importance and need for resilience of such solutions and work with regulators and business to secure harmonised and pragmatic guidance that reflect these principles common to OECD members. Such collaborative work will increase trust and regulatory certainty by resulting in greater transparency and understanding of how governments fulfil their shared commitments to protecting privacy. This effort is critical to help develop durable and scalable solutions that address current obstacles to the trusted cross-border flow of data around the world.

As CDEP observed in its December 22 statement, "[e]stablishing trust and minimising disruptions in data flows is a fundamental factor in reaping the benefits of digitalisation." We strongly support this work and stand ready to provide relevant input or evidence to assist with your evaluation of existing practices or development of policy guidance for trusted government access to data.

Supporting organizations

Asociación Latinoaméricana de Internet (ALAI)

BSA | The Software Alliance

Business at OECD (BIAC)

Cámara Nacional de la Industria Electrónica, Telecomunicaciones e Informática, Mexico (CANIETI)

Coalition of Service Industries (CSI)

Computer & Communications Industry Association (CCIA)

Developers Alliance

DIGITALEUROPE

European Telecommunications Network Operators' Association (ETNO)

Global Data Alliance

Information Technology Industry Council (ITI)

International Chamber of Commerce (ICC)

New Zeeland Tech Alliance (NZTech)

Slovak Republic National Union of Employers (RUZ)

Social & Economic Research Institute of Malaysia (SERI)

Software & Information Industry Association (SIIA)

US Chamber of Commerce

US Council for International Business (USCIB)