BUSINESS at OECD

The OECD Process to Develop Common Principles for Trusted Government Access to Data:
BIAC Supports Continuation and Successful Completion of the Process with Timely Outcomes[1]

Draft 2.0 for Discussion Only

November 29, 2021

1. *Business at OECD* (BIAC) reiterates our strong support for the OECD process

Business at OECD (BIAC) reiterates our strong support for the OECD Committee on Digital Economy (CDEP) initiative to develop high-level policy guidance for trusted government access to personal data held by the private sector. As expressed in our statements from 7 April 2021, and 6 July 2021, the lack of such principles has contributed to eroding trust in cross-border data flows, with detrimental societal and economic impacts. The operations of organizations of all sizes, across all sectors around the world, could be disrupted, at a time when inclusive economic recovery is top of mind for every government. It is essential that OECD members are able to drive this process to successful completion.

The OECD has already demonstrated its unique convening power, by bringing together privacy, national security, and law enforcement experts from 23 countries, conducting successful evidence-based dialogues, and gaining consensus on essential safeguards for obliged access. We commend the significant progress that has been achieved thus far.

As an organization of like-minded countries, and one that embeds multistakeholder consultation in its policy processes, the OECD has an opportunity to be the first to set impactful and practical baseline international standards and norms for trusted government access to personal data, including public sector data, held by the private sector. This would set a firm foundation to further progress on Data Free Flow with Trust.

We note the October 2021 Global Privacy Assembly resolution on Government Access to Data, Privacy and the Rule of Law that highlights key privacy principles when governments access personal data held by the private sector for national security and public safety purposes. We also refer to the recent G7 Trade Ministers' Digital Trade Principles, which observed that consensus from OECD members on trusted government access to data would provide additional transparency and legal certainty in cross-border data flows, and drive positive economic and social impacts. The resulting principles, similar to the OECD Privacy Guidelines and the OECD AI Principles, which were both informed with extensive multistakeholder inputs, would influence global policy frameworks and national regulations on government access to data, and operationalize OECD members' shared commitment to protecting the fundamental

[1] This paper was developed by the *Business at OECD* (BIAC) Drafting Group on Government Access to Data Held by the Private Sector, which is comprised of *Business at OECD* CDEP Committee Members from across sectors and regions.

rights articulated in the International Covenant on Civil and Political Rights, to which each member state is a party.

BIAC appreciates the need raised by some governments to address direct access as part of this process[2]. We encourage OECD members, together with relevant subject matter experts, to consider a range of different potential options for addressing principles applicable to direct access in a manner that would not significantly extend the timeframe of this work. For example, OECD members may consider whether such principles can be addressed via relevant examples that would illustrate how some existing draft principles on obliged access can apply in additional contexts. In addition, we also encourage OECD members to find ways to leverage complementary dialogues and to share visible progress with the public, including as interim committee reports, that can address ongoing business needs. BIAC is concerned that failure to agree on outputs from this process could signal that OECD members are unable to agree on a shared understanding for enabling Data Free Flow with Trust, which may embolden abusive practices by non-OECD governments.

In the remainder of this paper, we reinforce our earlier input with additional evidence on the urgent need to address obliged access. In addition, we share the business perspective on direct access and examples of how governments and the private sector are cooperating today to address disproportionate and indiscriminate access. In that context, ongoing dialogues on cybersecurity norms may be considered as complements to any future OECD discussion on norms for direct access. We provide these examples to encourage members to continue to work toward producing concrete and timely outputs, and we stand ready to offer support to enable progress on this very important initiative.

2. There is continued economic impact and urgent business need to address obliged access

The Court of Justice of the European Union (CJEU) decision in Schrems II[3] is an additional impetus for this OECD initiative since the subsequent uncertainties around EU-US data flows which have arisen from the ruling are due to conflicting principles related to government surveillance practices, which companies cannot unilaterally resolve. Business views the OECD process as not only a complementary dialogue to a trans-Atlantic data flow deal that is urgently needed, but also as an opportunity for a global dialogue that would, over time, lead to standards for Data Free Flow with Trust (DFFT). Like-minded governments should acknowledge

[2] The use of the term "*direct access*" in this statement refers to the discussion on different methods of government access to personal data held by the private sector in "*Government access to personal data held by the private sector: Update on the work of the informal drafting group, CDEP special session, 8 July 2021,"* Directorate for Science, Technology and Innovation, Committee on Digital Economy Policy, DSTI/CDEP(2021)8/REV1, 24 June 2021, as captured in Figure 1. Although there is no explicit definition of "*direct access"* in the document, BIAC interprets the use of this term by OECD members based on discussion with the Secretariat during consultations as referring to methods of government access other than "*obliged access"* or voluntary disclosures, and would include *"clandestine operations / covert access"* (from Figure 1) and "*signals intelligence and intercept, covert espionage operations and hacking"* (additional explanation from Annex B, paragraph 6).

[3] Court of Justice of the European Union (CJEU), Case C311/18 of July 16, 2020.

the importance and need for resilient solutions and work with stakeholders to secure harmonized, pragmatic and durable guidance that reflect common OECD values.

Cross-border data transfers are a key component of modern economies and international trade. The OECD (2020) recognised the U.S. and Europe as important global hubs for the import and export of digitally deliverable services[4]. In statements on 7 April, 5 May and 6 July, 2021, BIAC and its partners have consistently outlined concerns and evidence on the ongoing socio-economic impacts[5], globally, regionally and domestically, of eroding trust in cross-border data flows.

The economic value of safeguarding transatlantic data transfers cannot be understated. The data transfer relationship between the U.S. and EU is estimated to be worth $7.1 (€5.9) trillion[6]. The U.S. and Europe are seen as a "fulcrum of global digital connectivity" – being the two largest net exporters of digitally-enabled services to the world[7]. In 2019, the U.S. exported over $245 billion in digitally-enabled services to Europe and from which it imported an estimated $133 billion[8].

Decisions that safeguard international data transfers post-Schrems II could impact further economic opportunity in Europe. A recent study[9] indicates that the EU would be better off by €2 trillion by 2030 by safeguarding cross-border data transfers. The same study indicates that in a potentially negative scenario, where data governance restricts or makes EU data transfers to third countries unworkable and major trade partners restrict data flows, Europe would potentially lose out on €1.3 trillion growth by 2030, €116 billion in exports annually and 1.3 million jobs. Impacts would be cross-sectoral, affecting both large and small firms.

Uncertainties caused by lack of trust in government access to data can impede business opportunities to the same extent as data localization regulations and restrictions in cross-border personal data transfer, leading to significant GDP losses. As per an ECIPE analysis in 2014, the economic impact of mandatory data localization could result in a potential GDP loss of $100 billion in China; this is followed by the EU with a total estimated loss of $40 billion in the region[10]. Furthermore, the same study estimated that welfare losses (expressed as actual economic losses by the citizens) can amount up to $63 billion for China and $193 billion for the EU.

In addition, the impact caused by businesses that feel threatened by government access cannot

[4] OECD (2020) https://www.oecd-ilibrary.org/science-and-technology/perspectives-on-the-value-of-data-and-data-flows_a2216bc1-en;jsessionid=kIR7SLL0s_gZhGSqmjVPf6tx.ip-10-240-5-171.
[5] Impacts included enterprise, education and healthcare.
[6] U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows, 16 July 2020.
[7] Hamilton and Quinlan (2021), The Transatlantic Economy
[8] Hamilton and Quinlan (2021), Ibid.
[9] Digital Europe (2021), The value of cross-border data flows to Europe: Risks and Opportunities.
[10] Bauer, M., et al, The Cost of Data Localisation: Friendly Fire on Economic Recovery, ECIPE No.3/2014.

be ignored. In a recent survey of companies in ASEAN and India on DFFT[11], 33% of the respondents expressed concern in "government access" or "source code access" by the government – which is significant especially as it is comparable to the 29% that expressed concerns for forced data localization. This implies that not only China and the EU, but also Vietnam, Brazil, India, Indonesia, and South Korea will also be affected by the GDP loss of $1.5 to 6 billion each by government access.

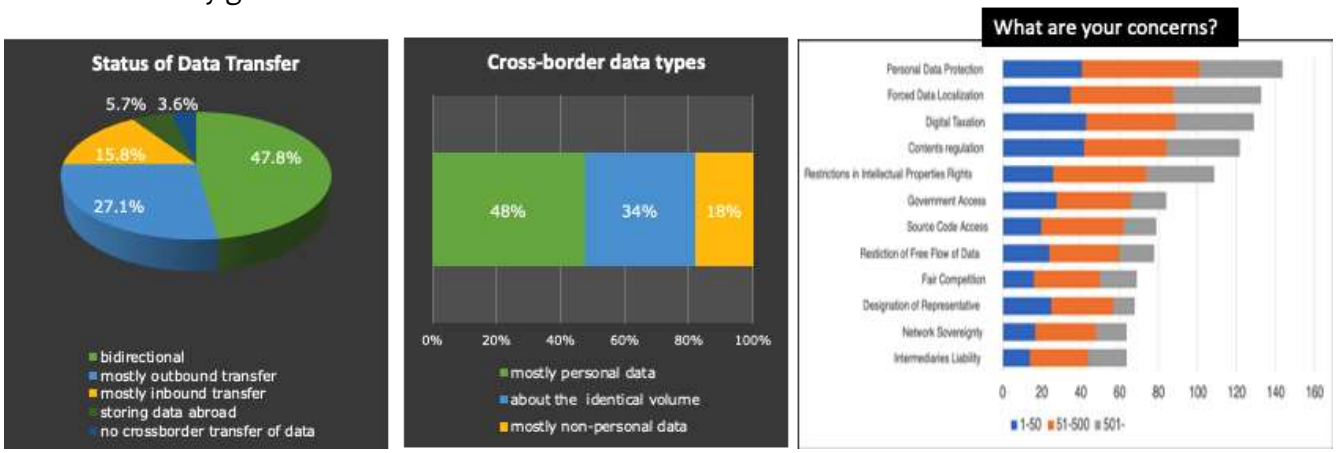

Figure 1. Data Free Flow with Trust Study in ASEAN+India region in 2021, by CFIEC, Center for International Economic Collaboration in Japan. Total 450 responses from Digital Industry; approximately 50 in each economy.

The societal and economic effects discussed here will only grow worse with every day of inaction and uncertainty in the ability of governments to access data held by the private sector, further impacting cross-border data flow. Timely actions and clear public signals from the OECD are essential as the process moves forward.

3. The path forward: a multi-phase process, building on the principles agreed in June 2021, and leading to standards for Data Free Flow with Trust (DFFT), with timely outputs and interim deliverables that can help to address priority issues with direct economic and social impact, prior to the OECD's 2023 timeline

BIAC strongly supports the OECD moving forward on this workstream in a manner that recognizes the many commonalities between OECD member countries.

The OECD has already convened a unique and substantive dialogue with a broad range of experts in national security, law enforcement, privacy, business, and civil society that has given it unique insight and perspective on these issues. As an organization of like-minded countries, the OECD has an important opportunity to recognize appropriate international standards and norms for trusted government access to data held by the private sector. The recognition of such standards can help restore trust to the legal frameworks within the OECD community,

[11] https://www.cfiec.jp/en/pdf/pr/interim-report-of-the-questionnaire-survey-2021-11-16.pdf.

which would advance DFFT and also distinguish the practices of its member countries from regimes that do not share these common principles. We encourage the OECD to move forward on this workstream in a manner that takes into account both the substantial expertise of the government drafting group and also the range of feedback provided by participants in the OECD's process.

BIAC notes the need expressed by some governments to address direct access as part of this process. If the OECD chooses to do so, we would encourage OECD members to ensure that these discussions are informed by their appropriate subject matter experts and to consider a range of options for addressing direct access in ways that would enable progress and not significantly extend the timeframe of this work, while leveraging complementary dialogues and sharing visible progress with the public, including as interim committee reports, that can address urgent business needs related to obliged access.

As BIAC noted in our statement dated 6 July 2021, the economic impact of direct government access is less well understood than obliged access. Because industry employs strong encryption and other security features to prevent direct access and is not involved in this form of access through compulsory process, direct government access to data has less visible impact on the business community's ability to harness cross-border data flows and promote economic growth. Yet a perception that direct access practices may be untethered to public standards or accountability can contribute to a lack of trust in cross-border data flows and negatively impact economic output. And the business community has long maintained a strong interest in establishing clear international principles and norms to address direct access in ways that protect human rights and provide a foundation for further international cooperation on cybercrime[12].

OECD members may also consider using counter-examples that illustrate malicious government intelligence operations that are clearly inconsistent with the values of OECD members and that fall well outside the bounds of OECD principles. BIAC notes that disproportionate and indiscriminate attacks like the SolarWinds cyber-attacks[13], or the "malicious cyber activities" and "irresponsible and harmful behaviour" in the attacks on Microsoft Exchange Servers[14] have already been condemned by multiple OECD member states[15]. These and other examples appear to reveal broad alignment among OECD members on shared safeguards to address state-actor cyber-attacks and data breaches targeting democratic institutions and values.

---

[12] For example, more than 1,000 businesses, governments, civil society and other organizations, including numerous OECD member states and members of the BIAC CDEP Committee, have endorsed the Paris Call for Trust and Security in Cyberspace – a set of nine principles that set out the responsible behaviour of State and non-State actors to promote norms and ensure peace and security in the digital space. *See* https://pariscall.international/en/.

[13] FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government | The White House.

[14] China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory - Consilium (europa.eu).

[15] Cases of cyberattacks including those by a group known as APT40 which the Chinese government is behind (Statement by Press Secretary YOSHIDA Tomoyuki) | Ministry of Foreign Affairs of Japan (mofa.go.jp).

One potential way forward would be to add on to the existing draft principles specific examples showing how some principles may apply to all forms of government access. This approach has the benefit of capitalizing on the strong work already done by the OECD's drafting group and ensuring the existing draft principles are retained. At the same time, this approach could also broaden some draft principles to provide a robust and comprehensive counter-point to countries that do not share the democratic values of OECD members, by illustrating how the principles may apply in additional contexts as well, while ensuring the rule of law is respected. Whether the OECD chooses this path or another alternative, however, we believe the most important outcome is for the OECD working group to move forward in recognizing a set of principles that is supported by all participants in the OECD process with timely interim deliverables for the public.

More broadly, we encourage the OECD to view this workstream as part of a multi-phase effort – and as an important contribution to the larger global conversation on government access to personal data. In our view, OECD principles on trusted government access to personal data could become a foundation for building trust in government access to data held by the private sector more widely. Indeed, we view the OECD's workstream as capable of having a strong influence on global policy frameworks and national regulations worldwide, in a manner similar to the OECD's Privacy Guidelines and AI Principles, which have set important baselines for global conversations on privacy and AI, respectively.

In the context of government access to personal data, like-minded members of the OECD could recognize principles on trusted government access to personal data that can similarly become the basis for long-term political and legal arrangements that support the continuance and development of international data flows. Such collaborative work can increase trust and regulatory certainty by resulting in greater transparency and understanding of how governments fulfill their shared commitments to protecting privacy.

4. BIAC is committed to successful completion of the OECD process, with timely and impactful outcomes

The OECD's effort to develop high-level principles for trusted government access to personal data held by the private sector is critical to establishing durable and scalable solutions that address obstacles to the trusted cross-border flow of data around the world. Such principles would also be a significant achievement for both CDEP and for the OECD broadly at showing the strength of the organization in convening these important discussions on pressing, global challenges and achieving concrete, impactful results. Much progress has already been achieved, and BIAC encourages the OECD to pursue timely and concrete outputs to address the urgent need. As we have since this workstream was first developed, BIAC stands ready to offer any support or evidence to enable progress on this critically important initiative.