BUSINESS at OECD

Business at OECD (BIAC) Statement on the OECD Committee on Digital Economy Policy's work to develop high-level principles or policy guidance for trusted government access to personal data held by the private sector

April 7, 2021

We commend the OECD Committee on Digital Economy Policy (CDEP) on its effort to bolster trust and minimize 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—such as child exploitation, human trafficking, drug trafficking, and serious violent and financial crimes—and in addressing national security threats—including terrorist attacks, espionage, the proliferation of weapons of mass destruction, and cybersecurity threats. OECD members also share a commitment to protecting the rights and freedoms of individuals, including the fundamental right to privacy.

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 such matters, and separately for businesses and internet users concerning the sufficiency of the protections that are guaranteed when their personal data is transferred to a third country or accessed by a third country's government. When governments lose sight of these common values, the cross-border free flow of data that is essential to domestic and multinational business operations and communications is restricted, and conducting business becomes costly and infeasible for organizations of all sizes across all sectors. Without a more predictable environment around global data flows, the pace of digital transformation will be slowed, impacting people and society at a time when economic recovery is top of mind for governments around the world.

Business at OECD (BIAC) looks forward to contributing our insights on the economic impact of the current lack of clarity, which governments are responding to by placing technically burdensome—and in some instances infeasible—restrictions on data flows. We also strongly support and stand ready to assist the CDEP in your work to articulate principles and recognize important safeguards to ensure trusted government access to

personal data. We build on our September 2020 statement[1] and expand the discussion to include the need to address national security concerns and additional issues for the OECD to consider in this initiative and future work.

Economic impact of eroding trust in cross-border data flows

The benefits of trade depend on the trusted and uninterrupted flow of data between countries. Virtually no economic activity today can happen in national silos; instead, it depends on close interaction with commercial partners and customers in different countries. The processing and transfer of personal data underlie all of these exchanges, including remote work and virtual collaboration, distance learning, telemedicine, cybersecurity, the fights against cybercrime and child abuse online, fraud monitoring and prevention, anti-money laundering, the investigation of dangerous counterfeit products, and a broad range of other activities that relate to the protection of health, privacy, and security. These services, when secure and respectful of the protection of data, enable the digital ecosystem to function, businesses to provide critical products and services, and people to stay connected with friends, family and communities, as well as the causes they care about and the businesses they support and depend on. The data exchanges also enable governments to provide timely information and more effective services for their citizens, especially during times of crisis such as the pandemic.[2]

International collaborations on COVID-19 research and responses provide vivid examples of how data flows have enabled new discoveries, information sharing, and collaboration that have helped 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. In each of these areas, the ability of an organization or enterprise to respond to the pandemic depends on its ability to safely send data across international borders. Similarly, the pandemic showed how crucial global data flows, when secure and respectful of data protection, are to the economy, as companies of all sectors and sizes all over the world responded by transitioning their businesses to online-first or online-only, and their operations to remote work.

---

[1] *Business at OECD* (BIAC) Statement on Unlimited Government Access to Personal Data Held by the Private Sector, September 2020

[2] As recently described by the UK Minister of State for Media and Data: "*Our hyper-connected world is increasingly reliant on data transfers. Everyday conveniences such as GPS navigation, smart home technologies and content streaming services rely on data transfers. They have modernised our way of life, helped enable us to make informed choices and use our time more efficiently. The pandemic has also forced us to share data quickly, efficiently and responsibly for the public good. We saw this happen with the hospital trusts which shared lung scans to improve coronavirus treatment methods, and we are determined to use these lessons to capitalise on the potential of data. Flows of data across borders underpin almost all economic activity as well as vital scientific research. They help power effective law enforcement cooperation, national security capabilities and the delivery of public services. In 2018 the UK exported £190 billion in services delivered digitally and in 2019 investments in the UK tech sector soared to £10.1 billion—a £3.1 billion increase on 2018's figures and the highest level in UK history. In the financial sector, service providers analyse data generated across the world to detect patterns, identify and stop fraudulent transactions, and help combat other criminal behaviour. In health care it also supports the delivery of more cost-effective bio-pharmaceutical research, and the development of new life-saving treatments. From a personal perspective, data transfers have enabled us to stay connected to friends, family and communities*." Available at https://www.privacylaws.com/reports-gateway/articles/uk114/uk114datatransfers/.

At the same time, we have seen erosion of trust in international data flows due to concerns that personal data may lose protections when accessed by governments across borders, or that governments may lose access to data over which they claim jurisdiction when it is transferred. These increased concerns and reduced trust have led to uncertainty that may discourage the participation of individuals, businesses, and even governments in a global economy, and they have already encouraged measures that can negatively impact economic growth.

- **Economic impact of disruption to cross-border data flows on business operations, products and services:**

    - Global companies of all sizes in every industry rely on cross-border data transfers to conduct business, innovate, and compete more effectively. 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.[3] This value is shared by traditional industries like agriculture, logistics, and manufacturing, which realize 75% of the value of the data transfers.[4]
    - With 60% of global GDP digitized by 2022, and growth in every industry driven by data flows and digital technology,[5] disruptions in cross-border data flows will have broad reverberations that can lead to reduced GDP growth, reduced investments in local markets, job losses and consequently public welfare losses, and adverse impact on the local/national digital ecosystems—at a time when economic recovery is top of agenda for every government.
    - Transatlantic data transfers are particularly important. Data transfers to the EU account for about 50% of US data transfers, while data transfers to the US account for an even greater share of EU data transfers.[6] These data flows support the roughly $312 billion in annual US services exports to Europe.[7]

- **Concerns about government access to health data can weaken population health and increase healthcare cost:**

    - A recent survey showed that people expressed overall skepticism at governments' intentions and ability to protect personal health data.[8] As such,

[3] OECD, *Measuring the Economic Value of Data and Cross-Border Data Flows*, 297 OECD Digital Economy Papers 24 (August 2020).
[4] McKinsey Global Institute, *Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity* (May 2011).
[5] Hamilton, Daniel D., and Quinlan, Joseph P., *The Transatlantic Economy 2020* (2020), available at https://transatlanticrelations.org/publications/transatlantic-economy-2020/.
[6] BSA | The Software Alliance, *The Future of Transatlantic Data Flows* (September 23, 2020), available at https://www.bsa.org/files/policyfilings/bsa_transatlanticdataflows.pdf.
[7] Hamilton and Quinlan, *The Transatlantic Economy 2020*, p. iii.
[8] Ipsos-WEF Global Consumer Views on data privacy 2019, available at Ipsos-WEF - Global Consumer Views on Data Privacy - 2019-01-25-FINAL.PPTX [Lecture seule]: People expressed the highest level of trust in healthcare providers at 59%, but overall skepticism at governments' intentions and ability to protect personal data. The level of trust is lowest for foreign governments at 20%, and only 39% trusts their governments to use personal data "the right way," with those in economically advanced countries having the least knowledge about authorities' access to and usage of personal data.

unlimited government access to personal health data could adversely impact people's health, leading them to avoid or forgo necessary medical treatment, or in some cases turn to informal "grey market" providers for fear that sensitive health conditions could be disclosed to the government. This would worsen individual clinical outcomes and general population health, and might foster emergence of a parallel illicit healthcare economy.

- Health services supply chains are complex and increasingly global. The COVID-19 pandemic highlighted global interdependencies for the supply of medical goods and the vast economic and human costs of their disruption. In a similar way, disruption of cross-border health data flows would impact the quality and cost of health care, jeopardizing the seamless provision of healthcare for individuals, potentially leading to poorer clinical outcomes and worse patient experience, while increasing healthcare costs.[9]

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

  - The number of measures that restrict cross-border data flow, as well as their restrictiveness, have been growing steadily globally, increasing the urgency of common approaches to trusted government access to data held or processed by the private sector.[10]
  - BIAC appreciates that the protection of fundamental rights of individuals must also be guaranteed in the context of promoting free data flows. However, some interpretations of the ruling of the Court of Justice of the European Union (CJEU) in *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (Schrems II) (C-311/18)* put pressure on organizations in the EU to localize data in the region. Although the CJEU's decision does not directly require localization of data or processes, it makes alternatives legally uncertain. The economic impact of such disruption to data flows could be severe, as recent data shows that 90% of EU-based companies from all economic sectors transfer data outside Europe, often to multiple countries, and that these transfers are predominantly used for business-to-business purposes.[11]
  - The European Data Protection Board (EDPB) responded to the *Schrems II* ruling by releasing draft recommendations on additional safeguards to be adopted when using Standard Contractual Clauses (SCCs), which is the instrument most widely used by private companies of all sizes and sectors to transfer personal data internationally. These draft recommendations are

[9] In a hypothetical example, a Dutch expatriate with a heart condition living in the UK could have information from his pacemaker sent to Germany and then shared with his physicians in the Netherlands and the UK, apply for experimental treatment in the US, discuss his claim with a nurse in the Philippines and have it processed in India, with his health data shared in real time securely between his payor and providers in different jurisdictions. These arrangements ensure the best quality of care for the individual, with a timely and cost-effective delivery of healthcare workflows through the leverage of centres of excellence and economies of scale.

[10] Ferracane, M., *Restrictions on Cross-Border data flows: a taxonomy*, ECIPE working paper No. 1/2017, available at Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf (ecipe.org); Ferracane, M>, and van der Marel, E., *The Cost of Data Protectionism*, ECIPE (October 2018).

[11] See DIGITALEUROPE, *Schrems II Impact Survey Report*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2020/11/DIGITALEUROPE_Schrems-II-Impact-Survey_November-2020.pdf.

intended to apply also in the event of new SCCs which are currently under negotiation by the European Commission.

- The EDPB draft recommendations have received significant criticism from the private sector, academics and governments (including nine EU governments in a December 2 letter) as the practical effect of these draft recommendations, if read strictly, would be to severely limit companies' abilities to conduct cross-border data transfers, and, in some cases, to preclude those transfers altogether.[12] If applied in their current form, these draft recommendations would impede the conduct of ordinary business activity. Currently, there is no comparable transfer mechanism to SCC under European data protection law which would be immediately available to businesses transferring data outside the EU.
- Similarly, regulatory enforcement actions pursued by some European Data Protection Authorities in the way they interpret the CJEU's ruling have raised questions about the durability of SCCs as legal mechanisms to enable the international flow of personal data. This comes at a time when the SCCs are themselves being revised and updated and other regions are exploring the use of contractual clauses as a stable mechanism for data transfer.

- **Compelled data localization requirements can be counterproductive in practice:**

  - Governments are increasingly considering or implementing data localization measures, either through legislation or soft law requirements. Where businesses must localize data for reasons that are unrelated to delivering their products and services locally as efficiently as possible, such measures are difficult to justify and often counterproductive, as they undermine global value chains and business operations across all industries. The ability to safely transfer data across borders is critical to the success of companies in sectors as diverse as agriculture, healthcare, manufacturing, banking, travel and hospitality, e-communications (including but not limited to social media), e-commerce, software, and many others. Compelled data localization frustrates the ability of companies to operate in multiple jurisdictions, making it difficult to manage hiring and human resources functions from a single headquarters, to evaluate the performance of connected vehicles from a single research hub, analyze cybersecurity threats at different points in communications networks, and to conduct reasonable network management functionalities, among other challenges.[13]

---

[12] See the December 2nd letter sent by government ministers and senior officials from the Czech Republic, Denmark, Estonia, Ireland, Lithuania, Poland, Romania and Sweden stating that "Overly restricting data flows would hurt the international competitiveness of our manufacturers and service providers and hinder the development of new digital business in Europe. It would also be seen as justifying the protectionist policies of a number of third countries, despite the very negative impact these policies already have on European companies." This letter is available at https://www.gov.pl/attachment/547ad1c7-c496-4eaf-8426-0a89ba360b78.

[13] See, e.g., Global Data Alliance, The Cross-Border Movement of Data: Creating Jobs and Trust Across Borders in Every Sector, available at[GDAeverysector.pdf (globaldataalliance.org)]; *Cross-Border Data Transfers and Supply Chain Management*, available at [Cross-Border Data Transfers & Supply Chain Management (globaldataalliance.org)].

- De facto localization requirements or compelled data localization may have unintended consequences for companies operating in those jurisdictions. Companies that operate in multiple countries may have to consider whether they can provide or continue to provide services in a particular jurisdiction, given the technical implications and costs involved. These concerns are compounded by potential implications for privacy that may arise from putting in place infrastructure that is specific to an individual country. Similarly, companies that operate in a single jurisdiction may be prevented from accessing global products and services, and may effectively be cut from global supply chains and, crucially, from foreign markets, stunting their growth and potential. This fragmentation of the internet undermines the economies of scale that is at the core of the digital transformation, including the enablement of micro, small and medium-sized enterprises and the growth of innovation ecosystems domestically.
- Across all industries, the deployment of technical measures broadly and irrespective of the context of a transfer to attempt to limit government access to data can curb the benefits and functionality of a globally interconnected business. Such measures can prevent companies from offering a broad array of features that are critically important to consumers, such as cybersecurity measures or improved communications functionality that depend on the ability to process the underlying data in multiple jurisdictions. These technical measures can also prevent the analysis of data originating from multiple sources in a way that leads to global insights and conclusions, such as combining personal data originated in different countries to implement global safety improvements and increase efficiency.
- Security of data is best achieved at scale with economies of scale arising from investment in robust security protections that apply to cross border data hosting. Per country data localization solutions cannot achieve those same economies of scale and encourage the use of low-cost solutions that would be sub-optimal given their limited scope. Such national digital borders further result in worse privacy and security outcomes for individuals.
- Data mirroring mandates similarly increase the cost of doing business in a jurisdiction by requiring companies to keep a duplicate copy of data in country. These mandates may assuage local authorities' fears that they will not have timely access to data that is needed in a criminal investigation if it is transferred beyond the state's borders. These measures, however, may also have the underlying goal of ensuring unrestricted and direct access by local authorities, compromising privacy rights and compounding the security risk.
- Ultimately, compelled data localization is not a solution to resolve the existing conflicts of law that often prevent companies from responding to a foreign government's legitimate law enforcement requests. Instead, compelled data localization is likely to exacerbate those conflicts and put businesses in an impossible position of arbitrating international legal conflicts, shifting the onus of insufficient regulatory alignment across democratic nations to the private sector.

- There is also a risk that compelled localization may be used as a tool by governments less committed to the protection of human rights to suppress freedom of expression, privacy, and other fundamental human rights.
- Restrictions on the free flow of data can be accompanied by limitations on the capacity of foreign law enforcement agencies to obtain personal data through lawful requests, which may frustrate governments' law enforcement efforts.
- Requiring data localization in specific circumstances may reflect a government's perception that it helps meet the law enforcement and national security needs of the country, such as to try to guard public sector data from access by a third-party government. However, as stated above, the movement toward compelled data localization is ultimately counterproductive toward those and other policy goals, and stunts the growth of country's economy and the broader digital economy.

- **Broader impacts from a lack of trust:**

    - 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 demand access to data over which they previously maintained exclusive control, further eroding trust and burgeoning the negative economic impact.

The OECD is an appropriate forum for resolving uncertainty surrounding trusted government access to personal data

By recognizing principles shared by OECD members on trusted government access to personal data held by the private sector, the CDEP can reinforce the strong traditions of OECD members in respecting the rule of law, alleviate uncertainty around governmental access to personal data held by the private sector, and ultimately help to expand trust in trade and digital technologies.

BIAC agrees with the 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. For example, we recognize that OECD members have strong traditions of respect for the rule of law, and their legal frameworks provide safeguards that limit the scope of demands for personal data and the use of any acquired personal data, with judicial approval or oversight constituting a central feature of such frameworks. This protection of fundamental rights of individuals must be guaranteed in the context of promoting free data flows. 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. We anticipate that the CDEP will find more commonalities than differences over the course of this analysis.

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 provide additional considerations for safeguards in the Annex, building on BIAC's previous statement from September 2020.

Once that foundation is firm, we encourage like-minded governments to recognize 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 harmonized 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 fulfill 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.

In the future, the OECD should also consider extending its work to address trusted government access to non-personal data—such as addressing the concerns and fears concerning potential access to research and industrial data and source code—as part of its work on a broader coherent data policy framework, further enhancing trust in the global digital transformation.

As the CDEP observed in its December 22 statement, "[e]stablishing trust and minimizing disruptions in data flows is a fundamental factor in reaping the benefits of digitalization." 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.

# # # # #

ANNEX

Business at OECD (BIAC) Supported Recommended Safeguards On Trusted Government Access to Personal Data

Business at OECD (BIAC) strongly supports OECD's recognition of safeguards on government access to data held by the private sector that are common to OECD member countries. We stand ready to provide relevant input or evidence as you bring together and elaborate a set of common and coherent good practices and legal guarantees from across OECD countries. Below we set out considerations for implementing the seven safeguards identified by the OECD Committee on Digital Economy Policy (CDEP) in its December 2020 statement on government access to personal data held or processed by the private sector. We offer these considerations as ways to further develop those safeguards in a manner that reconciles law enforcement and national security needs with protection of individual rights. These considerations build on BIAC's September 2020 statement addressing Unlimited Government Access to Personal Data Held by the Private Sector: Impact on Cross Border Data Flows and Economic Growth[14].

SAFEGUARD #1: Legal bases upon which governments compel access to personal data

- The rules, laws, and international agreements that allow for government access to data should be clear and consistent as to the types and categories of data and the authorities empowered to access it. The legal and regulatory frameworks should be publicly available and developed through processes that are open, transparent, and with opportunities for meaningful multi-stakeholder input.
- International agreements should advance frameworks that minimize conflicts of law and create mechanisms to resolve conflicts that do arise.

SAFEGUARD #2: Access to personal data tailored to meet legitimate aims

- The purpose and reach of government access to personal data should be limited to meet specific public safety and national security needs, as reflected in national laws, international law, and other appropriate sources.
- Demands based on national security authorities should be limited to defined purposes, such as counter-terrorism, counter-proliferation, promoting cybersecurity, and combating transnational criminal threats. Demands should not be used to violate, or have the substantial effect of violating, individuals' fundamental rights, or be used to acquire commercial advantage or data held by foreign governments or the public sector.

SAFEGUARD #3: Transparency

- *Related to the use of authorities:* The public has a right to know how, when, and why governments seek access to their data. Governments should issue regular detailed public statistical reports on the exercise of their powers to access personal data, including cross-border data demands. Companies should also be

[14] *Business at OECD* (BIAC) Statement on Unlimited Government Access to Personal Data Held by the Private Sector, September 2020

permitted to publish detailed statistical reports on demands they receive, including information about national security demands in the aggregate.

- *Related to notice to owner of data*: Individuals have a right to know when law enforcement seeks access to personal data.
    - Absent narrow circumstances, individuals and organizations should be provided with notice regarding law enforcement requests for their personal data. These narrow circumstances include when disclosure is not practical due to the existence of an emergency, or an ongoing investigation where disclosure will lead to the destruction of evidence, tampering with witnesses, or threats to public safety.
    - While notice is often impractical in the national security context based on legitimate operational security considerations, notice should be afforded when a national security demand for data leads to a criminal prosecution, the need for secrecy has expired, or whenever doing so is practicable.
    - To enable this notice, every effort should be made by governments to first obtain data from the data subject to whom the data relates or from the data controller who interacted with the data subject. This will further enhance transparency around government access requests.

SAFEGUARD #4: Approvals for and constraints placed on government access

- Government access should be narrowly tailored and subject to robust independent oversight mechanisms and bodies.
- Public sector data routinely includes individuals' highly sensitive health and financial information, and other personal data. Providers are subject to data access laws around the world and governments should not place providers in the middle of government on government demands for public sector data collection.

SAFEGUARD #5: Limitations on handling of personal data acquired, including confidentiality, integrity and availability safeguards

- Governments must require strict and transparent data minimization and retention and dissemination limits when they seek access to personal data of both citizens and foreign persons. Personally identifiable information, such as personal health data, should be handled in ways that provide adequate privacy protection. Principles contained in the OECD Privacy Guidelines, including use limitation, security safeguards, and accountability, remain relevant in the context of law enforcement and national security.
- Governments must also establish clear limits on the purposes for which collected data may then be used, including prohibitions on the use of data to suppress dissent or free expression, or target an individual for further surveillance or investigation based on race, ethnicity, nationality, religion, disability, sexual orientation, gender, or gender identity.

SAFEGUARD #6: Independent oversight

- Law enforcement demands of access to personal data should be predicated on prior independent review and approval (other than in duly substantiated cases of urgency). Government requests for personal data to protect national security,

including with respect to programmatic surveillance, should be subject to independent review and approval.

SAFEGUARD #7: Effective redress

- Individuals, organizations, and providers impacted by a government access request should have clear mechanisms through which to challenge unlawful or inappropriate surveillance demands or collection practices, or to raise conflicts of law, in front of an independent authority, such as the judiciary, an independent administrative body, or other body consistent with the legal traditions and authorities in a given country.

# # # # #