To: Prime Minister Narendra Modi

Cc: Shri Arun Jaitley, Minister of Finance
Dr. Jitendra Singh, Minister of State
Dr. Urjit Patel, Chairman of the Reserve Bank of India
Ajay Prakash Sawhney, Secretary of the Ministry of Electronics and Information Technology
Shri Suresh Prabhakar Prabhu, Minister of Commerce and Industry
Dr. Gulshan Rai, National Cyber Security Coordinator of the National Security Council Secretariat

Date: 20 November 2018

Re: Data Localization Requirements in India's Draft Privacy Law and Reserve Bank of India Circular on Electronic Payments

The Global Services Coalition (GSC) represents the services sector in Coalition member economies on issues of international trade and investment. We write to express our serious concerns in relation to the Indian Government's apparent increasing use of mandatory data localization requirements, including the Reserve Bank of India's April 6, 2018 Directive requiring that all data relating to electronic payment systems be stored locally in India, as well as the data localization requirements contained in the 2018 Personal Data Protection Bill (PDPB). The increasing reliance of all economic sectors on mobile technology, internet platforms and digitally enabled services has made cross-border data flows the lifeblood of global trade and investment. Data flows are the building blocks of technological advances such as cloud computing, the Internet of Things, Artificial Intelligence and the rapidly evolving services and technologies of the Fourth Industrial Revolution. GSC members acknowledge the challenges of rapidly increasing data flows, and recognize that it is essential to ensure appropriate data security and effective protection of personal data. However, the GSC believes that cross-border data flows need not be impeded, and that any exceptions should be limited to legitimate public policy

objectives, be non-discriminatory in their operation, and comply with the General Agreement on Trade in Services (GATS) Articles XIV and XIV bis.

India is an important market for GSC member businesses. India also has major IT and computer companies which are significant actors in the global digital economy, with a strong interest in supporting its competitiveness and growth. Data localization requirements and other policies that restrict data flows are likely to constrain growth and innovation, and reduce the scope for leading Indian IT firms and their GSC counterparts to engage in business and investment contributing to promoting India's competitiveness and growth. According to a 2014 report by the European Centre for International Political Economy (ECIPE), widespread data localization requirements in India could lead to a 2 percent decrease in foreign investment into India, cost the average Indian worker as much as 11 percent of their monthly salary, and result in welfare losses of as much as $14 billion.[i]

There are also likely to be some specific, possibly unintended, effects. For instance, as the proposed rules would apply to all personal data processed within India, they could in fact cover personal data collected from residents of foreign jurisdictions and sent to India for processing. As many organizations outside India rely on Indian-based companies to process foreign personal data, the application of Indian privacy rules to the processing of such data in India would impose an added layer of regulation, discouraging the use of Indian-based service providers. The proposed rules need scrutiny, with such effects in mind.

Nor is there any evidence that data localization enhances data security. Indeed a 2018 Brookings Institution study concluded that data localization can weaken rather improve data security. The study found that data localization prevents businesses from adequately ensuring data resilience, data recovery, and business continuity by severing connections to global data centers and hence to the protection from cyber threats that global data centers are designed provide.[ii]

The Government of India need not rely on data localization requirements to address its data privacy and security concerns. For example, the APEC Cross-Border Privacy Rules (APEC CBPR) provide a useful voluntary set of privacy principles that can guide data protection practices and procedures. Major global markets with large digital trade flows such as Japan, Australia, and Singapore also have a wide range of legal processes to govern cross-border data transfers such as accountability, binding corporate rules, contractual clauses, and consent. GSC members appreciate the importance of the Indian market and its potential to become a vibrant digital hub. We therefore strongly urge you to recognize the costs and potential adverse impacts of data localization measures for all businesses, including Indian exporting firms, and to turn to alternative regulatory approaches that can ensure data privacy and security while facilitating cross-border data flows.

Sincerely,

Australian Services Roundtable, http://australianservicesroundtable.com.au
Canadian Services Coalition, http://chamber.ca/advocacy/canadian-services-coalition/
Coalition of Services Industries, https://servicescoalition.org/
European Services Forum (ESF), www.esf.be

Hong Kong Coalition of Services Industries, http://www.hkcsi.org.hk/
Japan Services Network, http://www.keidanren.or.jp/en/
BusinessNZ, https://www.businessnz.org.nz/
Taiwan Coalition of Services Industries, twcsi.org.tw
TheCityUK, https://www.thecityuk.com/

[i] Bauer, M. et al (2014), The Costs of Data Localization: Friendly Fire on Economic Recovery. European Center for International Political Economy (ECIPE).
[ii] Meltzer, and P. Lovelock (2018). Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia. Brookings Institution.