To,

Shri N. S. Vishwanathan
Deputy Governor
Reserve Bank of India

Shri B.P. Kanungo
Deputy Governor
Reserve Bank of India

Smt. Nanda Dave
Chief General Manager
Department of Payment and Settlement Systems
Reserve Bank of India

June 22, 2018

Dear Shri.N.S. Vishwanathan, Shri. Kanungo, Smt. Nanda Dave,

BSA | The Software Alliance (BSA)[1] is the leading advocate for the global software industry, which creates cutting edge technologies that drive the global economy. Our member companies invest substantially in India and look forward to continuing doing so.

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation, and Workday.

Le-Meridien
15th Floor, Room 1529
Windsor Place, Janpath
New Delhi 110001
India

P (91 11) 4978 9066
W bsa.org

We are, however, seriously concerned that the Directive on **'Storage of Payment System Data'** (Directive)[2] issued by the Reserve Bank of India (RBI) on April 06, 2018, which imposes data localization requirements, will have an adverse effect on the Government of India's efforts to foster the digital economy in the country according to the objectives set forth on the Digital India strategy enunciated by the Hon'ble Prime Minister Shri Narendra Modi. We, therefore, respectfully request the RBI to suspend implementation of the Directive until an open and comprehensive consultation with the stakeholders (including the industry) is conducted and alternative solutions, such as potential adjustments in reporting mechanisms, are duly considered.

The Directive requires payment systems operators to store '*entire data relating to payment systems*' only in India. "Data" is defined very broadly and the scope of the Directive is unclear. The Directive, therefore, may affect not only the payment processors but also companies providing services to payment processors.

Unfortunately, there was no public consultation before the Directive was issued. However, we infer that the purpose stated by the Directive to "ensure unfettered supervisory access to data" means RBI wishes to ensure it is able perform its regulatory duties. The Directive also mentions the need to ensure data integrity (security). We understand and support these objectives. However, neither localization of the data nor localization of the infrastructure is necessary to achieve these goals.

BSA member companies have a deep and long-standing commitment to protecting personal data across technologies and business models all over the world. Our members recognize that users are only comfortable taking advantage of the benefits of new technologies if they trust that they will not lose control over their personal data. We, therefore, support balanced policies that protect personal data and further cybersecurity.

For the reasons explained below, data and infrastructure localization mandates will not improve RBI's access to information, enhance the performance of its regulatory duties, or increase cybersecurity.

We share the views below to assist your efforts to implement a policy that will meet RBI's underlying regulatory objectives while allowing payment processing activities to leverage the benefits of cross-border data transfers. This approach will result in the availability of better and more cost-efficient services to the Indian market, and ensure the security of the data such servers handle.

[2] Storage of Payment System Data: https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0 last accessed: June 12, 2018

The RBI's Ability to Perform its Regulatory Duties Does Not Require Data and/or Infrastructure Localization

As mentioned above, we infer that one of the goals of the Directive is to ensure that RBI has access to information it needs to perform its regulatory duties. We agree that this is an important objective. The prohibition to store or otherwise process information abroad would not, however, advance this goal.

RBI should consider alternative, less restrictive mechanisms, to ensure its access to the information it needs while allowing data to be transferred across borders. Such an approach will increase cost-efficiency and cybersecurity. A solution, which could include adjusting payment processors reporting requirements, could be reached through a consultation with industry.

In order to provide payment processing services, providers are already obligated to comply with reporting requirements to RBI, allowing it to perform its regulatory functions. This obligation is not affected by the location where the information is stored.

When payment processors utilize third party services to perform their activities, they retain control of the data and have access to it as needed. It would be desirable that on We recommend that, along the lines of the 'Working Group report on Cloud computing option for Urban Cooperative Banks' of October 2012,[3] payment processors be obligated to ensure that they maintain their fiduciary responsibilities. The payment processors must factor in the risks of outsourcing data and implement suitable safeguards by way of contractual provisions to ensure information is properly protected and accessible regardless of where data is stored or otherwise treated or processed.

Even other financial regulators who have considered this issue have concluded that data residency requirements are unnecessary — in part because such requirements provide very few benefits, but also because they inhibit competition and the choice of technology that may be best suited to the financial institutions' needs. In November 2017, the Brazilian Central Bank (BCB) proposed the 'Regulation on Cybersecurity Policies and the Procurement of Data Processing, Data Storage, and Other Cloud Computing Services' (Regulation), which would have prohibited organizations regulated by the BCB from procuring cloud services that involve data storage or other types of data processing outside Brazil. BSA submitted comments[4] to the

[3] Working Group Report on Cloud Computing Option for Small Size Urban Cooperative Banks https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/RWGFUF031012.pdf; last accessed: June 22, 2018

[4] BSA Comments on the Brazilian Central Bank http://www.bsa.org/~/media/Files/Policy/Data/11212017CommentsonCentralBankRegulations_English.pdf last accessed: June 22, 2018

BCB on the proposed regulation urging that the data localization requirements be eliminated. Our recommendations were duly taken into consideration by the BCB and data localization requirements were eliminated from the final Regulation. Institutions regulated by the BCB will be allowed to procure cloud services from companies that store data outside Brazil as long as they comply with the requirements.

Financial services regulations in both Hong Kong and Singapore expressly permit data held by financial services institutions ("FIs") to be stored and processed outside of the country, subject to certain conditions. These conditions range from general responsibilities to ensure that access to data and regulatory oversight are not impacted by the transfer. to specific obligations to ensure that the regulator has contractual rights to audit the service provider. By imposing these conditions, the regulatory authorities are satisfied that the storage and processing of FI data outside of the country will not impede their access to data or their ability to perform their oversight activities in a timely manner.

We strongly recommend that RBI work in consultation with industry representing payment processors, financial institutions, cloud service providers (CSPs), and others to adopt similar solutions to achieve its regulatory objectives whilst continuing to support innovation and choice in the financial sector industry in India.

By requiring that data is hosted within India, RBI will eliminate many data storage options from those available to its regulated entities. Even where a particular provider may have hosting facilities in India, it is likely that some of the functionality it can provide will require that data is stored outside of India because of how such platforms are configured. It is simply not practical for providers to have all of their services and functionality available in every country. Part of the cost savings and efficiencies that CSPs are able to offer result from economies of scale which often require data be stored in multiple locations.

Data and Infrastructure Location Restrictions Weaken Cybersecurity

The Directive states that payment systems "necessitate adoption of safety and security measures, which are best in class, on a continuous basis." Data security is, in fact, very important.

Data security is ultimately not dependent on the physical location of the data or the location of the infrastructure supporting it. Security is instead a function of the quality and effectiveness of the mechanisms and controls maintained to protect the data in question. Companies consider many factors when deciding where to locate digital infrastructure such as servers and gateways, including maximizing Internet speed and access, implementing redundancy and backup capabilities, and ensuring the deployment of state of the art security solutions for user

data. Data localization requirements prevent regulated institutions from enhancing security by backing up data in multiple locations that are in different regions.

Therefore, requiring localization of servers in India puts data at risk. Prime Minister Modi has championed the cause of a 'Digital India' and has also echoed sentiments of India playing a big role in cybersecurity globally.[5] This Directive sets a poor precedent by promoting practices that threaten data security.

Moreover, many service providers with excellent security may not be able to provide their services exclusively using data centers located in India. Data residency requirements would exclude those providers and prevent the use of solutions that offer strong security in India.

BSA appreciates the opportunity to share these preliminary views and we reiterate our request that RBI suspend the implementation of the Directive until full consultation with stakeholders takes place. This consultation will enable RBI to consider alternative solutions to achieve its purposes that do not include data localization mandates. The consultation process would also help ensure future polices are clear regarding their scope and implementing mechanisms.

Best regards,

Mr. Venkatesh Krishnamoorthy
Country Manager
BSA | The Software Alliance

Cc:
Shri. Ajay Prakash Sawhney, Secretary, MeitY
Shri. S. Gopalakrishnan, Joint Secretary, MeitY
Shri. Subash Chandra Garg, Secretary, Department of Economic Affairs
Shri. Prashant Goyal, Joint Secretary, Department of Economic Affairs
Shri. Gulshan Rai, National Cyber Security Coordinator, National Security Council Secretariat, Prime Minister's Office.

[5] Prime Minister's remarks during launch of Digital India Week July 01 2015 Source: https://www.ndtv.com/india-news/digital-india-pm-modi-says-india-can-play-a-big-role-in-cyber-security-globally-777319