November 24, 2020

National People's Congress
No. 23, Xijiaominxiang
Xicheng District, Beijing 100805
The People's Republic of China

Re.: Draft Personal Information Protection Law

The undersigned organizations represent companies of all sizes and from a broad range of industry sectors headquartered in Australia, Asia, Europe, North and South America. Many of these organizations and the companies they represent are concerned about various provisions of the draft Personal Information Protection Law (draft PIPL). Such concerns are being communicated to you through different channels and we respectfully ask you to consider them. This letter focuses on our specific concerns regarding the data localization requirements included in the draft PIPL and we are grateful for the opportunity to share these comments.

Many of the companies we represent rely on international data transfers to better serve Chinese customers. The ability to transfer data across borders is particularly relevant as many companies are

engaging in activities to help stop the progression of the Covid-19 pandemic in countries around the world and to contribute to economic recovery in China and globally.

The draft PIPL (Article 40) requires critical information infrastructure operators and personal information processors transferring "personal information reaching quantities provided by the State Cybersecurity and Information Department" to store that information in China. This is a clear expansion of the scope of "critical information infrastructure" (CII) that does not adequately consider how CII is referenced in other related laws and regulations such as the Cybersecurity Law and the draft Critical Information Infrastructure regulation. The draft PIPL extends well beyond the data localization requirements of the Cybersecurity Law, which are reserved only for CII. In addition, there is also no clear definition of what constitutes a "large volume" of personal information that would trigger the requirement. Furthermore, the focus of legal requirements should be on ensuring companies take proper measures to protect data and not on the amount of data transferred by any given organization.

Limitations on the cross-border transfer of personal data in the form of data localization or other highly restrictive requirements do not advance data protection goals. Data localization and data transfer restriction requirements may also trigger unintended consequences. These include limiting the access of local companies and customers in China to many innovative services and products. Additionally, as noted above, limitations on international data transfers may impede Covid-19 response and recovery efforts. Companies in China and elsewhere continue to play an important role in these global efforts but these efforts would be hampered if companies were not able to responsibly transfer data from China to other countries.

The implementation of security measures by companies that are responsible stewards of data may also be negatively impacted by data localization mandates. First, storing data at geographically diverse locations can enable companies to reduce network latency, maintain redundancy and resilience for critical data in the wake of physical damage to a storage location, and obscure the location of data to reduce the risks of physical attacks. In addition, cross-border data transfers allow for cybersecurity tools to monitor data traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. Cross-border data transfers are therefore essential to cybersecurity.

Our member companies support policies that protect personal information while enabling data to move across borders. Organizations that transfer data globally should implement procedures to ensure that when data is transferred to countries other than where it was collected, the data will continue to be protected. Responsible data stewardship is based on the principle that personal data controllers (which are akin to "personal information processing entities" in the draft PIPL) should protect data regardless of where the data is located. This accountability approach, which was first established by the OECD, was subsequently endorsed and has been integrated in many legal systems including the EU, Japan, New Zealand, Singapore, Canada, and Brazil, just to name a few. The accountability principle is also a significant feature of the APEC Privacy Framework and the APEC CBPR system. The adoption of robust, accountability-based mechanisms, such as the contractual safeguards and certification schemes referenced in Article 38, would be consistent with international standards and best practice. They would also render data localization unnecessary to achieve data protection objectives.

We welcome Article 38's reference to certification and contractual clauses as permissible methods for transferring personal information outside China, as these mechanisms are contained in other data protection legal systems. Meeting any one of these requiments should be sufficient to allow data to be transferred outside China. Article 39, however, further requires personal information processors (akin to data controllers in other legal systems) to separately obtain consent from individuals before data transfers can take place. We strongly recommend not imposing consent as an additional requirement

when other basis for transfer such as contractual clauses can be relied upon because this would be duplicative , costly, and would deviate from international best practices without increasing data protection. Conversely, in cases when consent is obtained, it alone should also be considered sufficient basis for transferring data to other countries

For the reasons outlined above, we encourage you to reconsider the requirements for data localization, as well as provide clarity regarding data transfer mechanisms and key terms used in the draft PIPL.

Sincerely,

American Chamber of Commerce in China

Associação Brasileira das Empresas de Software – ABES

Association of American Publishers – AAP

Australian Services Roundtable

Australian Information Industry Association – AIIA

Asia Cloud Computing Association – ACCA

Biotechnology Innovation Organization – BIO

BSA | The Software Alliance

Coalition of Services Industries – CSI

European Publishers Council – EPC

Global Data Alliance – GDA

Information Technology Industry Council – ITI

Japan Electronics and Information Technology Industries Association – JEITA

Japan Information Technology Services Industry Association – JISA

The Software & Information Industry Association – SIIA

The International Association of Scholarly, Technical and Medical Publishers – STM

US-China Business Council – USCBC

United States Information Technology Office – USITO