THE US-CHINA BUSINESS COUNCIL
美 中 贸 易 全 国 委 员 会

USCBC Comments on the Second Draft Personal Information Protection Law

May 28, 2021

On behalf of the 240 members of the US-China Business Council (USCBC), we appreciate the opportunity to submit comments on the second draft of the Personal Information Protection Law (hereby referred to as "the Draft") to the National People's Congress. We appreciate efforts to increase protections of personal information and offer clear guidelines for businesses.

USCBC received comments from companies across diverse sectors that are impacted by the Draft. We appreciate the Draft's emphasis on establishing a strong privacy regime by articulating standards for personal information collectors, processors, and handlers. It also provides guidance on best practices in the event of data breaches and outlines basic requirements regarding consent to data collection.

USCBC and its member companies would like to encourage the lawmakers to incorporate feedback on multiple issues that could impact US businesses, particularly areas that have been left unchanged from the previous draft. In particular, we would like to highlight the following suggestions:

- **Consistency with international norms:** To the degree possible, we urge lawmakers to strive for consistency with other international frameworks. This will promote smooth implementation for multinational companies complying with personal information protection requirements across multiple jurisdictions and facilitate both strong privacy protections and healthy growth of the business community.
- **Data localization requirements:** The data localization requirements included in Article 40 of the Draft are not consistent with other international frameworks, including the EU's General Data Protection Regulation (GDPR) and the US's California Consumer Privacy Act (CCPA). These requirements should be reconsidered, as they are counterproductive to public and private sector interests. They risk curtailing industry growth and compromising the effectiveness of cybersecurity and risk management controls. We strongly recommend this requirement be removed. Furthermore using volume based thresholds to impose data localization requirements is not a meaningful method to determine risk, given that given that companies collect many different types of personal information, which carry different levels of risk

- **Cross-border data transfers:** Article 38 clause 3 requires that a standard contract provided by the CAC must be signed between sender and recipient for cross-border transfer of personal information. We recommend that this requirement be deleted or that a standard contract is suggested by the CAC that is in line with international norms, for example, the EU's Standard Contractual Clauses. If such a contract is proposed, we request a 24-month transition and an opportunity for the public to provide feedback on the proposed standard contract.
- **Legal basis for personal information collection:** Article 13 specifies that consent is the primary legal foundation for collecting personal information. USCBC suggests adding additional exceptions to the consent requirements, including "legitimate interests" and/or use cases for due diligence, legal claims, personal reference, and security as well as the processing of the business contact information. "Legitimate interests" serve as a basis for personal information collection in many jurisdictions, including Singapore, Brazil, and South Korea. These exceptions will provide greater operational capacity for businesses navigating an increasingly complex data environment.
- **Vague grounds for separate consent:** Article 24 requires personal information processors to obtain recipient-by-recipient consent when data is shared with any "other party." This article will prove burdensome to implement, as businesses may regularly need to share data among their own subsidiaries or public authorities. Obtaining consent on a case-by-case basis will not be feasible in many instances where the personal information processor is already relying on other legal foundations to access the information (e.g., contractual obligations or other legal obligations). To resolve this hurdle, USCBC suggests that Article 24 specify conditions under which disclosure to a third party without separate consent is permissible. These could include when disclosure is necessary to fulfil contractual, legal, public health, or emergency obligations. Additionally, we recommend that individuals receive notification of categories of recipients, rather than individual names. This approach will prove less burdensome to businesses and also provide users with more actionable and informative information on how their data is used. This is consistent with precedent established with the EU's GDPR and is more user friendly for both the individual and the data processor.
- **Onerous notification requirements:** Article 56 requires notification to authorities and impacted individuals for all data breaches. This threshold is too low and would likely result in over-reporting, creating undue burdens for both regulators and the business community. We recommend adopting a risk-based approach, and require mandatory notification only where there is the potential for significant risk of harm to the impacted individuals. Such an approach would also allow organizations and regulators to focus resources appropriately on matters of material risk.