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

**USCBC Comments on the Draft Provisions on Regulating and Facilitating Cross-Border Data Flow**

October 13, 2023

On behalf of the over 270 members of the US-China Business Council (USCBC), we appreciate the opportunity to provide comments to the Cyberspace Administration of China (CAC) on the draft Provisions on Regulating and Facilitating Cross-Border Data Flow (hereby referred to as "the Draft"). We appreciate the CAC's efforts to relax requirements on outbound data flows, which will contribute to improving business sentiment for multinational companies that conduct business with China. We are grateful for the CAC's efforts to maintain transparency and its consideration of industry perspectives during this process.

USCBC and its member companies encourage the CAC to fully consider industry feedback on areas of the Draft that stand to impact US businesses operating in China. The Draft is a welcome step, but we encourage additional clarity and exemptions in order to reduce the operational burdens on companies. There remain several areas of ambiguity, which could impose barriers on companies. In particular, we would like to highlight the following key points:

**1. Clarify relationships among articles**

- Articles 1 to 7 provide a variety of exemptions for security assessments. It is critical to clarify how these exemptions interact with each other. For example, the volume thresholds articulated in Articles 5 and 6 should only count personal data records that are not covered by the exclusions set forth elsewhere in the Draft.

**2. Treatment of sensitive personal information**

- It remains unclear whether the exemptions and numeric thresholds outlined in the Draft are applicable to sensitive personal information governed by the Personal Information Protection Law (PIPL). The Draft should clarify the treatment of personal information and sensitive personal information.

**3. Inconsistency with existing laws**

- The Draft could conflict with existing laws, such as the PIPL, Cybersecurity Law, and Data Security Law. We recommend aligning existing laws and regulations with the Draft to reduce inconsistencies.

**4. Greater clarity and examples regarding exemptions**

- For exemptions outlined in the Draft, we encourage more examples listed so as to provide greater clarity for companies on what scenarios qualify as exemptions. For instance, it is unclear whether the exemption included in Article 4(1) applies to the cross-border transfer of customers' personal information for multinational businesses in the hotel and airline industries.

**5. Uncertainty for existing submissions**

- The Draft should clarify how companies that already submitted outbound data security assessments to provincial or central CACs should proceed. We recommend the Draft should offer specific guidance or a mechanism for companies. If the Draft is not adopted before the existing measures on data export security assessment go into effect, companies are forced to choose between facing more compliance risk or bearing significant cost to pass the data export security assessment.

**6. Lingering questions on important data**

- We encourage regulators to adopt a consistent definition and classification of "important data." Additionally, it remains unclear what the Draft means by relevant departments or regional administrations, and such notification by these authorities should be written and not verbal only. We also recommend if a company receives notice that their data is classified as important data, outbound data security assessments should be prospective, not retroactive.

**7. Ambiguity surrounding negative lists**

- We encourage the issuance of a national-level Negative List. We also recommend requiring Free Trade Zones (FTZs) to adopt negative lists that are consistent with, and no more restrictive, than any national-level Negative List, as this will ease compliance burdens for businesses. Otherwise, companies that operate in multiple jurisdictions may be required to adhere to inconsistent rules. We also seek clarity on when such lists will be issued.

**8. Numeric thresholds remain burdensome and unclear**

- We encourage regulators to increase the numeric threshold from 10,000 to 100,000 individuals, providing more companies with exemptions from all security assessment requirements when exporting personal information. Low thresholds do not adequately ease the operational burdens on companies. We also encourage additional clarity on how thresholds will be applied to companies that have multiple subsidiaries in China.

**9. Consistency with international norms**

- To the degree possible, we urge regulators to strive for consistency with other international frameworks. For example, if a standard contract for cross-border transfer is required, we recommend the CAC to align its requirements with those of the European Union's Standard Contract Clauses, where registration is not required but must be presented to the regulator upon request.

| Article | Content | Comments | Suggestions |
|---|---|---|---|
| 1 | Outbound data flows generated from international trade, academic cooperation, multinational manufacturing and marketing activities, which do not involve personal information or important data, do not need to apply for outbound data security assessment, enter a standard contract for cross-border transfer of personal information, or obtain a personal information protection certification. | 1) We recommend adding international financing, multinational provision of services, multinational business cooperation and communication, and international events and conferences, which do not involve personal information or important data, as exemptions.<br>2) We also recommend adding cross-border payment information, remittances, and travel and lodging information as further exemptions. The purpose of these processing activities is to provide services to citizens and residents in China, which have strong business needs.<br>3) We seek clarity on whether corporate data, not important data, is exported as a part of activities relating to international trade, financing, international banking, and contains information of the corporate's contact person, authorized person, director, beneficial owner, personal guarantors, etc., constitutes personal information? | Outbound data flows generated from international trade; **international financing**; academic cooperation; multinational manufacturing; multinational marketing activities; **multinational provision of services**; **multinational business cooperation and communication; operational components; and international events and conferences** which do not involve personal information or important data, as well as transfers of cross-border payment information, cross-border remittances, and cross-border travel and lodging information, do not need to apply for outbound data security assessment, enter a standard contract for cross-border transfer of personal information, or obtain a personal information protection certification.<br><br>**Information of corporate's contact person, beneficial owner, director, supervisor, management, authorized person, guarantors is corporate information, and shall not be deemed personal information.** |
| 2 | If relevant departments or regional administrations have not notified or publicly announced that the data is important data, the data processors | 1) We seek clarity on what relevant departments or regional administrations are. Additionally, what | If relevant departments of the State Council or the people's governments at the regional and provincial levels have not notified data processors or publicly |

| | | | |
|---|---|---|---|
| | are not required to submit outbound data security assessment applications for the data they processed as important data. | is the form of notification and are both written and oral notification included?<br>2) We also recommend if a company receives notice their data is important data, outbound data security assessments should be prospective, not retroactive. It should be prospective from the date that data processors receive the official designation of their data as important data.<br>3) We also encourage the consistent definition and classification of "important data." According to Article 2, we understand different regulators and regions have the discretion to decide and release their own catalogue of "important data." | announced that the data is important data, the data processors are not required to submit outbound data security assessment applications for the data they processed as important data. **Notification should be written and not only verbal. Important data's outbound security review should be prospective, not retroactive, from the date that the data processors receive the official designation of their data as important data.** |
| 3 | Personal information that is not collected and generated within the country does not need to apply for outbound data security assessment, enter a standard contract for cross-border transfer of personal information, or obtain a personal information protection certification when being exported abroad. | 1) We seek clarity on personal information collected overseas but subject to data processing within the territory, which could change the data security level or sensitivity. In this situation, is this personal information not subject to declare a data export security assessment, enter into a personal information export standard contract, or obtain a personal information protection certification?<br>2) There may be different interpretations on what "not collected and generated within the country" means. We encourage clarity on defining what | **Where** personal information **(a)** is not collected and generated within **the PRC or relates to natural persons not within the territory of the PRC, including where the personal information is further processed in the country; or (b) relates to foreign data subjects in the country, and where such personal information in (a) or (b) is transferred to foreign entities, personal information processors** do not need to apply for outbound data security assessment, enter a standard contract for cross-border transfer of personal information, or obtain a personal information protection certification |

| | | | |
|---|---|---|---|
| | | within the territory means. As a related point, when a consumer located in China engages in online shopping on a foreign marketplace, is this personal information generated within or outside the territory of China? We also seek additional exemptions for personal information that relates to natural persons not within the PRC. | when being exported abroad. **Further, if there is no additional personal information being transferred to foreign entities (e.g. authorization response to a cross-border transaction or a confirmation response to a database query), the above exemption shall apply.** |
| 4(1) | In any of the following circumstances, there is no need to apply for outbound data security assessment, enter a standard contract for cross-border transfer of personal information, or obtain a personal information protection certification.<br><br>It is necessary to provide personal information to foreign entities for the purpose of fulfilling a contract in which an individual is involved as a party, such as cross-border shopping, cross-border remittances, reserving flight and hotel, and visa processing. | We recommend clarifying the relationship between Article 4 and Articles 5-6. A lack of clarity will likely lead to confusion in the applicability of Article 4 and Articles 5-6, undermining the legislative purpose of Article 4 and the Provisions as a whole, inappropriately increasing compliance costs for businesses.<br><br>We recommend clarifying whether the scenario described as “reserving flight and hotel” applies to multinational corporations (MNCs) in the hotel and airline industries since the majority of personal data they collect and process are for the purposes of making flight and hotel reservations.<br><br>We suggest clarifying the scope "necessity for performing the contract” that qualify for exemptions by including more examples as below to illustrate when declaring a data export security assessment, entering into a personal information export standard | For personal information subject to Article 4, which is exempted from the requirements for declaring a data export security assessment, entering into a personal information export standard contract, or obtaining a personal information protection certification, it should not be counted into the volume-based thresholds of Articles 5 and 6.<br><br>We recommend exempting the cross border transfer of customer data which are collected by MNCs in the hotel and airplane industries without volume-based threshold restrictions.<br><br>We suggest including the following exemption criteria:<br>(a) Personal information of business partners' contact persons to overseas entities for the purpose of facilitating business communication for data processors. |

| | | | |
|---|---|---|---|
| | | contract, or obtaining a personal information protection certification is not necessary. We recommend keeping the scope reasonably wide to achieve desired effects of the Draft.<br>(a) To ensure effective business partnership with suppliers, distributors, and partners, transfer of their basic personal or work-related information of individuals acting as points of contact, such as their name, business contact phone number, business contact email, job title, and position should qualify for exemptions. This is critical to timely communication while involves less sensitive data that poses lower risk to the interest of individuals and national security.<br>(b) In the context of pharmaceutical R&D, cross border transfer of clinical data is an essential step for multinational pharmaceutical companies to establish multicenter clinical trials, conduct global pharmaceutical development, and submit drug registration applications. Ensuring the free flow of clinical data aligns with international best practices, we recommend referring to the Information Security Technology—Personal Information Security Specification, providing a certain degree of exemption for the use | (b) Necessary, de-identified personal information provided to overseas entities for scientific research or other research and development activities<br>(c) Personal information transfer in cross-border transactions for the purposes of fraud prevention or monitoring; or personal information for risk prevention and management,<br>(d) Personal information to overseas entities within a reasonable scope that individuals have voluntarily made public or has been legally disclosed through other means<br><br>Moreover, we recommend further clarity on if certain data is exempted from obtaining separate consent based on PIPL, then no additional consent is required by the Draft. |

| | | | |
|---|---|---|---|
| | | of de-identified personal information for academic research purposes.<br>(c) Personal information transfer in cross-border transactions for the purposes of fraud prevention or monitoring or personal information for risk prevention and management, should be considered necessary for purposes of fulfilling relevant contracts.<br>In reference to Article 13 (1) of the Personal Information Protection Law (PIPL), it is suggested to include "providing personal information to overseas entities within a reasonable scope that individuals have voluntarily made public or has been legally disclosed through other means" as an acceptable scenario for exemption. This is beneficial for various industries, including the pharmaceutical sector, to facilitate international academic exchange, research publications, and more. | |
| 4(2) | Where it is necessary to provide personal information of internal employees to foreign entities to implement human resources management based on relevant labor regulations and lawful labor contracts signed collectively. | In addition to internal employees, multinational corporations (MNCs) often engage in human resources management functions that encompass the processing and exporting of personal information related to a broader spectrum of individuals. This includes job candidates, contracted workers, former employees, interns, and the family members of these individuals for welfare and benefits management purposes. Applying | We suggest changing this to read:<br><br>Where it is to provide overseas the personal information (including sensitive personal information) of individuals for the conclusion or performance of a contract to which the individual is a resource of the organization or for the implementation of an internal employee for human resources management purposes:<br>(1) internal employees |

| | | | |
|---|---|---|---|
| | | exemptions in these scenarios is crucial for enabling companies to maintain a global talent pool and ensure the competitiveness of Chinese job candidates on a global scale.<br><br>We also suggest clarifying that the exemption is extended to the transfer of employee personal information via enterprise cloud services or centralized management database for internal business management and event monitoring purposes.<br><br>As provided by Article 13 of the PIPL and Supreme People's Court's Judicial Interpretation on Several Issues about the Application of Laws for the Trial of Labor Dispute Cases, human resource policies formulated by a company through democratic process and duly announced to employees, can serve as the basis to ascertain the parties' rights and obligations. Therefore, we suggest that separate consent from individual employees is not required in the situation described by this provision and the requirement of being "necessary" can be deleted, so that the companies may process human resources data according to the human resource policies duly stipulated according to the relevant laws of China. | (2) interns;<br>(3) contractors dispatched by a third party;<br>(4) job applicants;<br>(5) above individuals whose contract has expired or been terminated; and<br>(6) family members of the above individuals.<br><br>In addition, we suggest adding provisions to allow transfer of the personal information mentioned above via enterprise cloud services or centralized data management. |

| | | | |
|---|---|---|---|
| 4(3) | In emergency situations where personal information must be provided to foreign entities in order to protect the life, health, and property safety of natural persons. | We suggest changing "必须 [must]" in this provision to "确需 [necessary]" given that " 必须 [must] " is not a legal term used in the Personal Information Protection Law. Changing it to "确需 [necessary] " ensures the alignment with Article 38 of the Personal Information Protection Law.<br><br>It is required to transfer transaction information overseas for centralized processing in order for potential fraud to be detected. Such fraud prevention purpose is crucial to protect the property and safety of natural persons. | In emergency situations where it is necessary to provide personal information to foreign entities in order to protect the life, health, and property safety of natural persons.<br><br>We recommend that crime and fraud prevention be clarified to be an "emergency situation" where the property of natural persons may need to be protected as well. |
| 5 | If it is anticipated that the personal information of fewer than 10,000 individuals will be transferred outside of the country within one year, there is no need to apply for outbound data security assessment, enter a standard contract for cross-border transfer of personal information, or obtain a personal information protection certification. However, when the outbound transfer of personal information is based on individual consent, the consent of the personal information subject should be obtained. | 1) We seek clarity on the definition within one year, particularly regarding the start time. We recommend one year refers to the next calendar year.<br>2) We recommend the volume thresholds exclude scenarios in Articles 1 to 4 so as to reduce the obligations on the multinational companies. The thresholds should only count those personal data records that are not covered by the exclusions.<br>If the same individual personal information will be transferred to different systems, will it be counted once or twice? Or in other words, is it counted as one piece of personal information or two? | If it is anticipated that the personal information of fewer than **100,000** individuals will be transferred outside of the country within the **next calendar year**, there is no need to apply for outbound data security assessment, enter a standard contract for cross-border transfer of personal information, or obtain a personal information protection certification. **These volume-based thresholds exclude scenarios outlined in Articles 1 to 4 of the Draft**. However, when the outbound transfer of personal information is based on individual consent, the consent of the personal information subject should be obtained. |

| | | | |
|---|---|---|---|
| | | 3) We recommend once data is transferred outside of China, it should not be double counted for subsequent years. For example, in Year 1, if 1000 records of specific individuals were transferred, in the Year 2, since these 1000 records are already present overseas (even if they continued to be transferred on an ongoing basis), the volume should only apply to any additional new records to be transferred beyond the initial 1000.<br>4) Does the rule treat individual personal information and individual sensitive information the same? In that regard, the draft should also clarify whether the thresholds apply to sensitive personal information processed by companies and organizations, such as employee and consumer sensitive personal information, rather than just those processed by Communist Party, Chinese government, and Chinese military.<br>5) We recommend the provisions clarify whether separate consent is required, as the PIPL requires data processor to obtain separate consent for personal information cross-border transmission.<br>6) We also recommend raising the minimum threshold from 10,000 to 100,000 to better balance the risks and | Additionally, we recommend the final language address issues related to double counting in subsequent years and whether the thresholds apply to individual subsidiaries or are cumulative. |

| | | | |
|---|---|---|---|
| | | needs of data flow. The low number plays a limited role in promoting data flow.<br>7) We also seek clarity on how to count the personal information of subsidiaries. For example, what if there are four subsidiaries who each have 10,000 pieces of personal information (cumulatively 40,000). | |
| 6 | If it is anticipated that the personal information of more than 10,000 individuals but less than 1 million individuals will be transferred outside of the country within one year, there is no need to apply for outbound data security assessment if a standard contract for cross-border transfer is established with the foreign recipient and registered with the provincial-level cyberspace administration department of personal information, or if a certification of personal information protection is obtained. However, when the outbound transfer of personal information is based on individual consent, the consent of the personal information subject should be obtained. If it is anticipated that the personal information of more than 1 million individuals will be transferred | 1) We recommend raising the threshold from 10,000 to 100,000 to better balance the risks and needs of data flow. Additionally, we are unsure if the threshold of 1 million individuals will effectively ease the burden on large multinational companies.<br>2) We seek clarity on how sensitive personal information will be treated.<br>3) We seek clarity on the definition within one year, particularly regarding the start time. We recommend one year refers to the next calendar year.<br>4) We recommend the volume thresholds excludes scenarios in Articles 1 to 4 so as to reduce the obligations on the multinational companies. The thresholds should only count those personal data records that are not covered by the exclusions.<br>For instances that require registering Standard Contracts for Cross-Border Transfers with the provincial level | If it is anticipated that the personal information of more than **100,000** individuals but less than 1 million individuals will be transferred outside of the country within the **next calendar year**, there is no need to apply for outbound data security assessment if a standard contract for cross-border transfer is established with the foreign recipient and registered with the provincial-level cyberspace administration department of personal information, or if a certification of personal information protection is obtained. However, when the outbound transfer of personal information is based on individual consent, the consent of the personal information subject should be obtained. If it is anticipated that the personal information of more than 1 million individuals will be transferred outside of the country within one year, it is required to apply for outbound data security assessment. However, when the outbound transfer of |

| | | | |
|---|---|---|---|
| | outside of the country within one year, it is required to apply for outbound data security assessment. However, when the outbound transfer of personal information is based on individual consent, the consent of the personal information subject should be obtained. | Cyberspace Administration Department of Personal Information, we recommend the CAC could further improve their requirements by aligning them with those of the European Union's Standard Contract Clauses, where registration is not required but must be presented to the regulator on request. This would greatly improve business efficiencies and remove any potential bottlenecks (as are being experienced under the current requirements). | personal information is based on individual consent, the consent of the personal information subject should be obtained. **These volume-based thresholds exclude scenarios outlined in Articles 1 to 4 of the Draft**. |
| 7 | Free Trade Pilot Zones may independently formulate a list of data (referred to as the "Negative List") that needs to be included in the applicable scope of outbound data security assessment, standard contract for cross-border transfer, and personal information protection certification within the jurisdiction of the Pilot Free Trade Zone. The Negative List needs to be approved by the provincial-level cyberspace administration department and then registered with the Cyberspace Administration of China. Outbound data flows that are not included in the Negative List do are not required to apply for outbound data security assessment, enter a standard contract for cross-border transfer of | 1) We encourage consistency among the Negative Lists as this will ease compliance for companies. Otherwise, companies that operate in multiple jurisdictions may be required to adhere to inconsistent rules.<br>2) We seek clarity on when the Negative List will be issued. We also recommend the Negative List should not be stricter than the Central CAC's standards. Additionally, we encourage FTZs to consult with resident companies when developing the data negative list and seek companies' feedback on the draft negative list before submitting to the provincial CAC for approval.<br>3) We also seek clarity on how the Negative List works in practice. For example, if a firm is headquartered in a FTZ and has subsidiaries in non-FTZ | We recommend the formulation of a national-level Negative List. |

| | | | |
|---|---|---|---|
| | personal information, or obtain a personal information protection certification. | cities, would the non-FTZ cities be included? We recommend equal treatment at headquarters and subsidiaries. We also recommend the Greater Bay Area is included as an FTZ. | |
| 8 | Government agencies and operators of critical information infrastructure that transfer personal information and important data to foreign entities should comply with relevant laws, administrative regulations, and departmental rules. When sensitive information related to the Party, government, military, and confidential units, as well as sensitive personal information are provided to foreign entities, relevant laws, administrative regulations, and departmental rules should be followed. | While Article 8 mentions obligations of critical information infrastructure operators (CIIOs) when transferring data oversea, it fails to address whether MNCs that serve those CIIOs will be subject to the same laws and regulations.<br><br>In addition, while Article 8 mentions "sensitive information" and "sensitive personal information," the rest of the Provisions fails to distinguish between these two categories of information which can lead to confusions. | We recommend adding explanation that the "personal information" referred throughout the article includes "sensitive personal information" unless otherwise regulated,<br><br>It should also be clarified whether the exemption thresholds in Articles 4-6 also applies to sensitive personal information processed by companies, organizations such as employee and consumer sensitive personal information other than those related to communist party, Chinese government and Chinese military. |
| 9 | Data processors that transfer important data and personal information outside of the country shall comply with the provisions of relevant laws and administrative regulations, fulfilling their obligations of data security protection, and | There is a lack of a threshold for security incidents, which could lead to overreporting. Companies need greater clarity on criteria that they can use to assess security incidents which can be followed by "increased risk." | We recommend that the regulation includes a threshold for cybersecurity incident reporting. Moreover, as financial institutions have existing cybersecurity incident reporting requirements imposed by financial regulators, we recommend inter-agency coordination between financial regulators and the CAC so that |

| | | | |
|---|---|---|---|
| | ensure the security of outbound data flows. In the event of security incidents of outbound data or when there is an increased risk to outbound data security, data processors shall take remedial measures, and report to the cyberspace administration department in a timely manner. | Moreover, there is duplication of cybersecurity incident reporting requirements between financial regulators and the CAC which may create confusion and undue burden on financial institutions. | regulated entities' report to financial regulators could fulfil the requirement in this regulation. |
| 10 | Local cyberspace administration departments should strengthen their guidance and supervision over data processors' outbound data transfer activities. Local cyberspace administration departments should enhance both proactive and reactive monitoring, and if they identify significant risks in outbound data transfer activities or if a security incident occurs, they should require data processors to rectify and eliminate the underlying issues. In cases where data processors refuse to correct their behaviors or if their behaviors lead to serious consequences, they should be legally ordered to cease data export activities to ensure data security. | Additional high-profile directive documents should be released by CAC to guide local cybersecurity administrations to streamline work procedures. This includes conducting reviews on previous experiences in data export security assessments and standard contract filings, optimizing the acceptance and evaluation processes and unifying and enhancing assessment criteria. | We encourage adding guiding opinions to require local cyberspace administrations to optimize their work procedures, promulgating manual guidelines, streamlining administrative process, and avoid arbitrarily adding bureaucratic procedures or raising processing thresholds. |

| | | | |
|---|---|---|---|
| 11 | In cases where relevant regulations such as Outbound Data Security Assessment Measures and Provisions on the Standard Contract for Cross-Border Transfer of Personal Information are inconsistent with the Provisions, the Provisions should be followed. | Companies are eager to obtain clarity regarding the resolution of legal conflicts that may arise due to discrepancies between this Draft and the outcomes of their data export security assessments. Adopting changes to their internal data processing and transfer models can be a costly process for companies. Therefore, any delay in announcing CAC's solution could result in significant financial losses that might ultimately prove unnecessary.<br><br>Given the changes in the transition from the previous to the new regulatory regime on data export, which may cause confusion for companies and potentially lengthen the time required for internal communication and restructuring, we suggest extending the remediation period, particularly for adjusting data export security assessment applications, by a minimum of six months.<br><br>We also seek confirmation that companies do not need to take action if they meet exemptions for not needing to apply for outbound data security assessment, enter a standard contract for cross-border transfer of personal information, or obtain a personal information protection certification as outlined the Draft. | We suggest providing data processors that already completed or are proceeding with data export security assessment prior to the implementation of the Draft is adopted with the opportunity to choose from the following options in accordance with the Draft:<br>1) reapply for data export security assessments if needed;<br>2) establish personal information outbound standard contracts if needed;<br>3) obtain personal information protection certification if needed.<br><br>Adjustments should be completed within six months from the date of this regulation's implementation. |