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

US-China Business Council Comments on the Draft Personal Information Protection Law

On behalf of the more than 220 members of the US-China Business Council (USCBC), we appreciate the opportunity to submit comments on the draft Personal Information Protection Law of the People's Republic of China (hereafter referred to as "the Draft") to the National People's Congress (NPC).

USCBC received comments on the Draft from companies across multiple industries, including information and communications technology (ICT), energy, manufacturing, and financial services.

The Draft serves as an important pillar of China's cybersecurity regime and defines the individual rights of persons over the processing of their personal information. Our membership is supportive of the Chinese government's objective to protect the privacy and security of persons within China, however, members have expressed concerns about provisions in the following areas:

1. **Extraterritoriality:** Article 3 states that the Draft applies to personal information processors outside of mainland China where analysis is being conducted on natural persons within China, or when the purpose of processing activities is to provide products or services to natural persons inside China. However, the terminology used to describe the scope of these activities is vague, making it challenging for companies to assess their compliance burden. This is exacerbated by a catch-all provision, which applies the extraterritorial elements of the Draft to "other circumstances provided in laws or administrative regulations."
2. **Unclear oversight:** Article 56 identifies the national-level Cyberspace Administration of China (CAC) as the leading regulator for personal information protection work, but also lists a multitude of unspecified regulators and government authorities who will have a role in enforcing the law. This unnecessarily increases the compliance burden for companies as they must work to identify appropriate authorities for reporting, and may have to send multiple incident reports to various authorities in the case of a data breach because it is unclear who is in charge.
3. **Undefined thresholds**: The Draft employs personal data volume thresholds to determine whether companies will be subject to cross-border data security reviews or whether they need to register as designated data protection managers with relevant authorities. However, volume by itself is not a meaningful indicator of risk, given that companies collect many different types of personal information, which carry different levels of risk.

Furthermore, the Draft does not define these thresholds, leaving companies unable to accurately assess their compliance requirements.

4. **Data localization**: Article 40 of the Draft mandates that critical information infrastructure (CII) operators and non-CII operators who process an unspecified volume of personal information will be subject to data localization requirements. This contradicts the *Cybersecurity Law*, which only mandates data localization for CII operators. Data localization makes data less secure by preventing it from being diffused along a global network. Localized data may be destroyed or made inaccessible in the event of an outage, limiting companies' ability to recover. Data localization may even be lead to a situation where companies located in the China are subject to more cyberattacks as attackers will be aware that they will gain access to massive amounts of localized data if they are successful. Most importantly, it is impractical and costly to require companies that offer services on a global scale to store and process their data locally. Localization requirements will ultimately discourage investment in the China market.
5. **Personal information collection rules:** The Draft does not explicitly allow the collection and processing of personal information on the basis of the "legitimate interests" of corporate entities. While Article 13 expands the legal bases for personal information collection beyond consent, there are no explicit exceptions to consent-based processing for employee personal data, which will prove unnecessarily onerous to companies as they try to manage employee training or access employee information from other jurisdictions.

We appreciate this opportunity to raise our suggestions, and have provided article-specific recommendations in detail below. The Draft's English translation is provided by New America.

List of Comments			
Article #	**Article/Clause**	**Comments**	**Suggestions**
Chapter I	General Principles		
3	This Law applies to organizations and individuals' handling personal information activities of natural persons within the borders of the People's Republic of China. Where one of the following circumstances is present in handling activities outside the borders of the People's Republic of China of	Members note that the extraterritorial elements of this article are overly broad and need more clarity to be implementable. Specifically, the terms "analysis" and "assessment," as referred to in Article 3.2 could be interpreted in a literal fashion to apply to anyone reading a news report of individuals based in the PRC. However, it is assumed that this article is meant to target big data analytics and profiling. The circumstance outlined in Article 3.3 functions as a catch-all that leaves companies unable to accurately assess their compliance burdens under the draft law.	We recommend narrowing the scope of Article 3.2 to "conducting analysis or assessment of activities of natural persons within the PRC's borders for the purpose of profiling using big data analytics." Additionally, we recommend eliminating Article 3.3 and providing exceptions for employee personal information handled by affiliates located outside the PRC and personal information collected for the purpose of business transactions.

	personal information of natural persons within the borders of the People's Republic of China, this Law applies as well: 1. Where the purpose is to provide products or services to natural persons inside the borders; 2. Where conducting analysis or assessment of activities of natural persons inside the borders; 3. Other circumstances provided in laws or administrative regulations.	Additionally, it is unclear how the draft law applies in the following scenarios: 1. Where the personal information of employees is processed by an affiliate located outside of China in accordance with agreements outlined in Articles 22 and 38. 2. When a company collects personal information for the purpose of conducting a transaction with a business located within the PRC (i.e., director's signature for a contract, contact information of a sales rep) but not for the purpose of offering a product or service as outlined Article in 3.1	

4	Personal information is all kinds of information recorded by electronic or other means related to identified or identifiable natural persons, not including information after anonymization handling. Personal information handling includes personal information collection, storage, use, processing, transmission, provision, publishing, and other such activities.	We welcome the broader definition of "personal information" included in this draft as it aligns with the definition outlined in the GDPR. Previous definitions presented in the *Cybersecurity Law* and *Civil Code* did not include "identifiable natural persons."	We recommend this article clarify whether pseudonymized or aggregated data is excluded from the scope of personal information.

8	In order to realize the handling purpose, the handled personal information shall be accurate and updated in a timely manner.	Due to the large amount of data that many companies handle, it will be burdensome for personal information processors to proactively ensure the accuracy of personal information provided to them. Data processors should be able to assume that the data provided to them is accurate.	We recommend that this article clarity that is the responsibility of the individual to ensure the accuracy of personal information they provide to personal information processors.

9	Personal information handlers shall bear responsibility for their personal information handling activities, and adopt the necessary measures to safeguard the security of the personal information they handle.	This article fails to distinguish responsibilities of "personal information processors" and "personal information controllers" and implies that all processors of personal information are subject to the same liabilities. This may conflict with agreements concluded with parties entrusted to process personal information as outlined in Article 22	We recommend adding an exception to this article for parties processing personal information under an entrustment with the personal information processor.

10	No organization or individual may handle personal information in violation of the provisions of laws and administrative regulations, or engage in personal information handling activities harming national security or the public interest.	The scope of activities which may endanger national security or public interest can be interpreted in an overly broad fashion.	We recommend providing clarity on what activities are considered to endanger national security and further recommend eliminating “public interest” from this clause.
Chapter II	Personal Information Handling Rights		

13	Personal information handlers may only handle personal information where they conform to one of the following circumstances: 1. Obtaining individuals' consent; 2. Where necessary to conclude or fulfill a contract in which the individual is an interested party; 3. Where necessary to fulfill statutory duties and responsibilities or statutory obligations; 4. Where necessary to respond to sudden public health incidents or protect natural persons' lives and	The draft law's expansion of legal bases for processing personal information beyond consent, as per the *Cybersecurity Law* and *Civil Code*, is a welcome liberalization. However, this article lacks provisions for the processing of personal information on the basis of the "legitimate interests of the personal information processor" which exists in international jurisdictions such as the EU's GDPR and Brazil's LGDP. This a necessary basis for legitimate processing activities in numerous scenarios including: ● Employer-employee relationships. For example, companies need to process personal data of employees for training purposes, and free consent cannot reliably be given by employees. ● The provision of services that entail the processing of personal data for individuals who are not parties in an agreement. For example, the provision of remote assistance to a truck driver may entail use of contact and geolocation data of drivers who are not a party in the service agreement stipulated between the manufacturer and the transportation company that owns the truck.	We recommend the inclusion of the "legitimate interests of personal information processors" to the enumerated legal bases, so long as such interests do not override individuals' rights and freedoms, or may be challenged by the individual. It is also recommended that "vital interests of the data subject" be introduced as a legal basis in order to further expand personal information processing legal bases beyond consent. Additionally we recommend clarifying that Article 13.3 applies to the fulfillment of duties or obligations under overseas laws and regulations given that this would enable financial institutions to meet their compliance obligations which are also monitored by PRC financial regulators. Finally, Article 13.5 should clarify what constitutes "reasonable scope."

	health, or the security of their property, under emergency conditions; 5. Handling personal information within a reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest; 6. Other circumstances provided in laws and administrative regulations.	Additionally the introduction of the "legitimate interests of the personal information processor" may also be used to provide companies legal certainty in circumstances where consent may be withdrawn such as when providing data to a third party (Article 24), cross-border transfers of personal information (Article 39), and disclosures of personal information (Article 26). Furthermore, it is unclear what constitutes the "reasonable scope" for personal information processing related to news reporting, public opinion and other activities outlined in Article 13.5. The subjective interpretation of "reasonable scope" may lead to the disclosure of more personal information than is necessary.	

14	Consent for handling personal information shall be given by individuals under the precondition of full knowledge and in a voluntary and explicit statement of wishes. Where laws or administrative regulations provide that specific consent or written consent shall be obtained to handle personal information, those provisions are followed. Where a change occurs in the purpose of personal information handling, the handling method, or the categories of handled personal information, the individual's consent shall be obtained again.	Requiring companies to re-obtain consent for every change in purpose, processing method, and categories of processed personal information will be overly burdensome. Furthermore the phrase "specific consent" (单独同意) as used in the Chinese text lacks clarity and definition.	We propose that this provision should not apply in scenarios where consent was not originally relied upon and the new purpose or change is compatible with the circumstances of the original processing activity. We also recommend that this provision be amended and clarified so that consent should only be re-obtained for activities where it was the original basis for processing. Finally the terms "consent," "written consent," and "specific consent" (单独同意) should be explicitly defined and their scopes clarified.

16	Individuals have the right to rescind their consent to personal information handling activities conducted on the basis of individuals' consent.	Compliance with other laws and regulations may necessitate the retention of personal data even in cases where consent is rescinded.	We recommend expressly stating that this article is subject to other laws and regulations.
18	Personal information handlers shall, before handling personal information, explicitly notify individuals of the following items using clear and easily understood language: 1. The identity and contact method of the personal	Requiring companies to proactively provide this level of information before processing personal information may prove burdensome. It seems unnecessary to do so in advance of an individual request. Additionally the definition and requirements of the term "store" in this article's final paragraph is unclear. It is unclear if this is a requirement for companies to make privacy notices publicly available with a "print" or "download" option. There is also a lack of clarity on what is meant by "before" as referred to in the first paragraph of this	We recommend making the notification described in this article available upon individual request, as opposed to companies proactively providing the notice before personal information is processed. Alternatively, requiring companies to have updated terms on a publicly available website instead of sending direct notifications is also considered reasonable. Additionally the term "store" in the final paragraph of this article should be deleted to prevent confusion.

	information handler; 2. The purpose of personal information handling and handling methods, the categories of handled personal information, and retention period; 3. Methods and procedures for individuals to exercise the rights provided in this Law; 4. Other items that laws or administrative regulations provide shall be notified. Where a change occurs in the matters provided in the previous paragraph, individuals shall be notified about the change.	article. Oftentimes data is provided (e.g., via email) before a notice can be sent.	

	Where personal information handlers notify the matters as provided in Paragraph I through the method of formulating personal information handling rules, the handling rules shall be public and convenient to read and store.		
21	Where two or more personal information handlers jointly decide on a personal information handling purpose and handling method, they shall agree on the rights and obligations of each. However, said agreement does not influence an individual's rights to demand any one personal information handler perform under this Law's provisions.	It is important to note that all joint arrangements will differ, and joint responsibility should not imply the joint liability of the various personal information handlers involved in the processing. On the contrary, the level of liability of each party must be assessed in accordance with the relevant circumstances of each case.	We suggest the following addition to the language: "Where personal information handlers jointly handling personal information harm personal information rights and interests, they bear joint liability according to the law and the relevant circumstances."

	Where personal information handlers jointly handling personal information harm personal information rights and interests, they bear joint liability according to the law.		
22	Where personal information handlers entrust the handling of personal information, they shall conclude an agreement with the entrusted party on the purpose for entrusted handling, the handling method, categories of personal information, protection measures, as well as the rights and duties of both sides, etc., and conduct supervision of the personal information handling	In a great deal of circumstances, an entrusted party will have specialized skills and capabilities for safeguarding personal information. As such, entrusted parties should be required to ensure that they have the necessary security measures in place and personal information processors should be able to rely on the entrusted parties obligation to maintain the security of the personal information where the personal information processors have performed proper due diligence.	To avoid confusion we recommend including a separate definition for the "entrusted party", and clearly define roles and responsibilities of processors and entrusted parties.

	activities of the entrusted party. Entrusted parties shall handle personal information according to the agreement; they may not handle personal information for handling purposes or in handling methods, etc., in excess of the agreement; and after the contract is fulfilled and completed or the entrusting relationship dissolved, return personal information to the personal information handler or delete it. Without the consent of the personal information handler, an entrust party may not further entrust personal information handling to other persons.		

23	Personal information handlers shall, where it is necessary to transfer personal information due to mergers, separations, and other such reasons, notify individuals about the receiving party's identity and contact method. The receiving party shall continue to fulfill the personal information handler's duties. Where the receiving side changes the original handling purpose or handling method, they shall notify the individual again as provided in this Law, and obtain their consent.	The requirement to obtain consent if the data is transferred to another legal entity is unworkable for many companies. Many companies often buy and sell portfolios/books of business, where it is not practical to obtain consent. Using the insurance industry as an example, failure to obtain consent under the circumstances outlined in this article would mean termination of cover and would be detrimental to the customers' interest.	We recommend removing the consent requirement outlined in this article or allowing a "legitimate consent" exception as per suggestions for Article 13. Additionally we suggest clarifying at what stage in the merger and acquisition (M&A) process is an individual notification to be sent. The need for confidentiality may also make it difficult to send out a notification before a M&A transaction has concluded.

24	Where personal information handlers provide third parties with the personal information they handle, they shall notify individuals about the identity of the third party, their contact method, the handling purpose, handling method, and personal information categories, and obtain the specific consent from the individual. Third parties receiving personal information shall handle personal information within the above mentioned scope of handling purposes, handling methods, personal information categories, etc. Where third parties change the original handling purpose or handling methods, they shall notify the individual again as provided in this	This article is likely to cause confusion and increase operational costs for the following reasons: 1. By requiring companies to obtain specific consent before the provision of their data to third-parties, this provision seems to contradict Article 13 of the draft law which provides multiple legal bases for processing personal information beyond consent. 2. It is recognized that the goal of this provision is to provide more transparency to data subjects for third-party data transfers. However it is impractical to require companies to notify individuals of the contact information, purpose, and methodology of each third-party, nor is it practical for third-parties to contact each individual for consent. Personal information processors already generally obligate the third-parties to safeguard personal information under instructions specified in contracts. 3. There are various business transactions that may result in the transfer of personal information from one party to the other, where it would not be practical for the	We recommend allowing the disclosure of personal information to third parties be permitted if any one of the requirements established in Article 13. 1. We propose that categories of recipients be notified rather than exact recipients, which is in line international norms, including the EU's GDPR. 2. The need for personal information handlers to obtain consent for third-party disclosures should also be eliminated when the personal information handler has already provided individuals details on third-party disclosures practices as part of their personal information processing practices. 3. An exclusion should be added for scenarios where personal information is entrusted to a vendor for processing.

	Law, and obtain their consent. Where personal information handlers provide anonymized information to third parties, third parties may not use technical or other methods to re-identify individuals.	recipient to contact individual data subject's for consent.	
25	When using personal information to conduct automated decision making, the transparency of the decision making and the fairness and reasonability of the handling result shall be guaranteed. Where an individual believes	It is unclear what objectively constitutes "fairness," "reasonability of the handling," and "rights and interests" as referred to by this article nor what constitutes a violation of these principles. Modern AI algorithms operate with an inherent level of uncertainty and inexplicability that makes complying with this provision difficult.	We recommend that there be exclusions to this article's obligations in any of the following scenarios: 1. Where consent has been given 2. When necessitated by contract 3. When it is otherwise lawful to do so Furthermore, we recommend that the guarantees referred to in the first sentence

	automated decision making creates a major influence on their rights and interests, they have the right to require personal information handlers to explain the matter, and they have the right to refuse that personal information handlers make decisions solely through automated decision making methods. Those conducting commercial sales or information push delivery through automated decision making methods, shall simultaneously provide the option to not target an individual's characteristics.		of this article only be provided in cases where the use of automated decision making (ADM) may produce a legal or significant impact on a data subject. Finally it is proposed that clarity be provided on what constitutes " rights and interests" as determined by this article. The above proposals are consistent with international norms, including the GDPR.
27	The installation of image collection or personal identity recognition equipment in public	Members note the challenge of obtaining consent from individuals when personal information is being processed in public spaces, as well as the need to process this data for insurance purposes	We suggest providing clarity on how consent is expected to be obtained under the scenarios mentioned in this article, and including alternatives to consent in

	venues shall occur as required to safeguard public security and observe relevant State regulations, and clear indicating signs shall be installed. Collected personal images and personal identity characteristic information can only be used for the purpose of safeguarding public security; it may not be published or provided to other persons, except where individuals' specific consent is contained or laws or administrative regulations provide otherwise.	(e.g., to assess liability in a slip and fall case on the premises of the insured) or to prevent fraud.	circumstances where it is not a viable option.

29	Personal information handlers may handle sensitive personal information only for specific purposes and when sufficiently necessary. Sensitive personal information means personal information that, once leaked or illegally used, may cause discrimination against individuals or grave harm to personal or property security, including information on race, ethnicity, religious beliefs, individual biometric features, medical health, financial accounts, individual location tracking, etc.		We recommend deleting "etc." within this article to limit the scope of sensitive personal information. In addition, we suggest that "individual location tracking" (个人行踪) should not be included as sensitive personal information.

30	Where handling sensitive personal information based on individual consent, personal information handlers shall obtain specific consent from the individual. Where laws or administrative regulations provide that written consent is obtained for handling sensitive personal information, those provisions are followed.	Within the scope of business activities conducted between two entities there are several scenarios where certain personal information is disclosed from one entity to the other where it would be impractical for the receiving entity to obtain consent from the relevant individuals for processing.	We recommend including a clarification allowing the receiving entity to process personal information based on the consent of the disclosing party. Furthermore we recommend that the disclosing party be responsible for obtaining individual consent for disclosure. Finally, we recommend an exclusion allowing for sensitive personal information to be processed without consent for the purpose of fraud prevention, and information security purposes.
Chapter III	Rules on the Cross-Border Provision of Personal Information		

38	Where personal information handlers need to provide personal information outside the borders of the People's Republic of China for business or other such requirements, they shall meet at least one of the following conditions: 1. Passing a security assessment organized by the State cybersecurity and informatization department according to Article 40 of this Law; 2. Undergoing personal information protection certification conducted by a specialized body	MNC companies with global operations often leverage their enterprise-scale information systems/strengths outside the borders of PRC for storing and processing of employee personal data from Chinese affiliates or subsidiaries. Without an exception for employee personal data, the proposed measures of this article will significantly increase the administrative burdens and operating cost of MNC companies unnecessarily. There is also uncertainty as to whether this provision applies to any personal information collected within China, or personal information that a processor may collect from outside of China but stores within its borders. However it should be noted that the ability to conduct cross-border data transfers on the basis of contracts with overseas recipients (38.3) is a well received liberalization.	1. We recommend the following: 1. Provide exclusions for the cross-border transfers of employee personal information. 2. Clarify that this article only applies to personal information that is collected within China. 3. Clarify whether the assessment mentioned in Article 38.1 is the same assessment described by the Draft Security Review Measures for the Cross Border Transfer of Personal Data.

	according to provisions by the State cybersecurity and informatization department; 3. Concluding an agreement with a foreign receiving party, agreeing on both sides' rights and obligations, and supervising their personal information handling activities' satisfaction of the personal information protection standards provided in this Law; 4. Other conditions provided in laws or administrative regulations or by the State cybersecurity and		

	informatization department.		
39	Where personal information handlers provide personal information outside of the borders of the People's Republic of China, they shall notify the individual about the foreign receiving side's identity, contact method, handling purpose, handling methods, and personal information categories, as well as ways for individuals to exercise the rights provided in this Law with the foreign	Typically, in most international laws including the GDPR, the transferring organizations are obligated to provide the details of the processing activity and information about the overseas recipients or categories of such overseas recipients. It does not prescribe what level of details are required. However, this article provides very prescriptive notice requirements for cross-border data transfers which include the overseas recipients' identities, contact information, as well as ways for individuals to exercise their rights provided with said foreign recipients. It is pertinent to note that today many MNC's share personal information with their foreign affiliates for processing or utilize third-parties outside of their	We recommend the following: 1. Combine Articles 38 and 39 such that transfers of personal information to entities outside the PRC is permitted when any one of the conditions listed in Articles 38 or 39 are met. 2. Categories of recipients should be notified instead of exact individual recipients. This is consistent with international norms, including the European Union's GDPR. 3. Eliminate the term "separate consent" in favor of the term "consent."

	receiving side, and other such matters, and obtain individuals' specific consent.	jurisdiction to carry out processing on their behalf. While providing names or categories of such overseas recipients or processors is reasonable, providing contact information is not necessary as it would only lengthen the privacy notice without serving any specific purpose. For any requests of access, deletion, correction, objection, etc., the individual should be required to make the requests only with the personal information handler, with whom they have a direct relationship. Individuals should not be allowed to have the option to exercise their rights with every party involved in the processing lifecycle as this could cause unnecessary confusion and complicate the entire process. Moreover, most parties would be contractually obligated to only act in accordance with the instructions of the personal information handler only. Additionally it is not clearly understood what is meant by "separate consent" as processors generally obtain an individual's consent to use and transfer their information at the same time.	4. Remove the requirement obligating personal information processors to provide the contact information of overseas recipients, and the ability for individuals to exercise rights with those recipients. 5. Clarify that the scope of this article is not inclusive of Article 38 and only applies to cross-border transfers of personal information that is not for business purposes.

40	Critical information infrastructure operators and personal information handlers handling personal information reaching quantities provided by the State cybersecurity and informatization department shall store personal information collected and produced within the borders of the People's Republic of China domestically. Where they need to provide it abroad, they shall pass a security assessment organized by the State cybersecurity and informatization department; where laws or administrative regulations and State cybersecurity and informatization department provisions permit that security assessment not be	This article extends data localization requirements beyond CII operators, as per the *Cybersecurity Law*, to non-CII operators that process an unspecified volume of personal information. However, requiring that certain data only be processed and stored locally would put individuals' and businesses' sensitive or proprietary data at greater risk of a security breach. This is because companies of all sizes use distributed networks, where data storage is spread out over servers in different locations -- often in different parts of the world. Furthermore, there are legitimate reasons for storing personal information outside the PRC, which do not compromise national security or individual's rights. For example, multinational organizations may need to transfer aspects of employee personal information to head offices to facilitate effective human resource planning and management. It is not practical to restrict the storage of personal information to the PRC in such situations. Finally, as currently written, this provision would need clarification on the data localization threshold to be implementable.	We recommend the following suggestions: 1. We suggest eliminating data localization requirements in favor of requiring operators to provide an adequate level of protection for data stored offshores. 2. Failing suggestion 1 the scope of data localization requirements should be limited to CII operators as per the *Cybersecurity Law*.

	conducted, those provisions are followed.		

41	Where it is necessary to provide personal information outside of the borders of the People's Republic of China for international judicial assistance or administrative law enforcement assistance, an application shall be filed with the relevant competent department for approval according to the law. Where the People's Republic of China has concluded or participates in international treaties or agreements that contain provisions concerning providing personal information outside of the borders of the People's Republic of China, those provisions are followed.		We suggest this article include exemptions for publicly available data, business contact data, and employee information.

Chapter IV	Individual Rights in Personal Information Processing Activities		
44	Individuals have the right to know and the right to decide relating to their personal information, and have the right to limit or refuse the handling of their personal information by others, unless laws or administrative regulations stipulate otherwise.	The reference to "right to decide" in the context of processing activities is unclear from the text and could be misconstrued.	We recommend providing an exception to this article for "legitimate business" interests. Additionally if the "right to decide" is in the context of allowing the individuals the right to choose whether or not they would want to consent to processing, we would recommend use of the term "consent" instead as the term "decide" may be misinterpreted.

45	Individuals have the right to access and copy their personal information from personal information handlers, except in circumstances provided in Article 19 Paragraph I of this Law. Where individuals request to access or copy their personal information, personal information handlers shall provide it in a timely manner.	Limitations to individuals' rights may be necessary, for reasons such as, but not limited to, protecting public interests, protecting the rights of other individuals and other legitimate reasons. Article 49 specifies that reasons must be provided to the individual if his/her request is rejected, which suggests an allowance for rejection of such rights. However, the lack of legal clarity may result in implementation challenges.	We suggest providing a list of exemptions where organizations may refuse a request from an individual. This list should include an exemption for when providing an individual access to copies of their data may result in violation of confidentiality agreements or the privacy rights of other individuals.

47	Personal information handlers shall, actively or based on individual requests, delete personal information where one of the following circumstances occurs: 1. The agreed retention period has expired, or the handling purpose has been achieved; 2. Personal information handlers cease the provision of products or services; 3. The individual rescinds consent; 4. Personal information handlers handled personal information in violation of laws, administrative	Implementing these provisions will be impractical when applied to employee personal information.	We recommend including exemptions for scenarios where consent may be withdrawn or including a specific exemption from this article for employee personal information.

	regulations, or agreements; 5. Other circumstances provided by laws or administrative regulations. Where the retention period provided by laws or administrative regulations has not expired, or personal information deletion is technically hard to realize, personal information handlers shall cease personal information handling.		

48	Individuals have the right to request personal information handlers explain personal information handling rules.		The law should explicitly provide for exemptions for processors to comply with requests when it is necessary to protect trade secrets or intellectual property.
49	Personal information handlers shall establish mechanisms to accept and handle applications from individuals to exercise their rights. Where they reject individuals' requests to exercise their rights, they shall explain the reason.		We suggest clarifying under what circumstances a personal information processor may refuse a data subject's request, and also suggest that a personal information processor may charge administrative fees to a data subject for copying or checking his/her personal information if the scope of checking and copying goes beyond reasonable requests.
Chapter V	The Duties of Personal Information Handlers		

51	Personal information handlers who handle personal information reaching quantities provided by the State cybersecurity and informatization department shall appoint persons responsible for personal information protection, responsible for conducting supervision of personal information handling activities as well as adopted protection measures, etc. Personal information handlers shall publish the name, contact methods, etc., of persons responsible for personal information protection, and report them to the departments fulfilling personal information		1. We recommend clarifying the personal information quantity threshold referred to in this article. 2. We suggest that the requirement to report/register the details of the designated data officer to relevant departments be made voluntary to avoid imposing undue costs and burdens on organizations.

	protection duties and responsibilities.		
52	Personal information handlers outside the borders of the People's Republic of China as provided in Article 3 Paragraph II of this Law shall establish a dedicated entity or appoint a representative within the borders of the People's Republic of China, to be responsible for matters related to the personal information they handle, and will report the name of the relevant entity or the name and contact method, etc., of the representative to the departments fulfilling personal information	The requirement to report/register the details of such representatives with the relevant regulatory authority can be cumbersome as representatives may change.	We recommend clarifying this article with exemptions aligned with the GDPR such that overseas controllers/processors need not designate a representative within China so long as their activity is occasional, does not include processing a large volume of sensitive personal information or is unlikely to result in a risk to the rights and freedoms of natural persons, etc. Furthermore we recommend that reporting/registration requirements be voluntary or removed entirely to avoid imposing unnecessary burdens on organizations.

	protection duties and responsibilities.		
53	Personal information handlers shall regularly conduct audits of whether or not their personal information handling operations, the protection measures they adopt, etc., conform to the provisions of laws and administrative regulations. The departments fulfilling personal information protection duties and responsibilities may require that personal information handlers entrust specialized entities to engage in audits.	The definition of "regularly conduct audits" and "entrust specialized entities" in this article is unclear. For most personal information processors, it is not necessary to conduct regular audits on personal information protection. Furthermore a mandated and sanction-based audit regime will degrade ongoing investments in cybersecurity and data protection.	We suggest that mandatory audits only be conducted for critical information infrastructure operators. Failing that, the frequency of the audits should be limited such that they do not unnecessarily increase operational costs for companies.

54	Personal information handlers shall conduct a risk assessment in advance of the following personal information handling activities, and record the handling situation: 1. Handling sensitive personal information; 2. Using personal information to conduct automated decision making; 3. Entrusting personal information handling, providing personal information to third parties, or publishing personal information;	This article suggests an overly broad range of activities where risk assessments will be required, including all processing of sensitive personal information, and any use of automated decision making (ADM). Regular business operations may also be caught by this article such as: 1. Sending employee data to a multinational organization's head office for employment management and employee benefits purposes, or 2. Outsourcing operational activities to vendors/service providers (e.g., engaging insurance companies for employee insurance purposes). These requirements are onerous and should be limited to high-risk scenarios where there is a material risk of harm to individuals.	We recommend the following: 1. This article should be revised to require risk assessments to be conducted, and records to be retained, for situations which are likely potentially result in high risk or material risk of harm to individuals. 2. Where ADM is concerned, we propose that the risk assessment be triggered only if the use of ADM "produces legal effects or significantly impacts an individual." This is in line with international norms, including GDPR.

	4. Providing personal information abroad; 5. Other personal information handling activities with a major influence on individuals. The risk assessment content shall include: 1. Whether or not the personal information handling purpose, handling method, etc., are lawful, legitimate, and necessary; 2. The influence on individuals and the degree of risk; 3. Whether or not the adopted security protection		

	measures are lawful, effective, and suited to the degree of risk. Risk assessment reports and handling status records shall be preserved for at least three years.		
55	Where personal information handlers discover a personal information leak, they shall immediately adopt remedial measures, and notify the departments fulfilling personal information protection duties and responsibilities and the individuals. The notification shall include the following items:	This article imposes reporting requirements to authorities/regulators and individuals for all data breaches, which would include accidental disclosures of non-sensitive personal information where there is no impact or risk of harm to individuals. This low threshold will result in over-reporting, and increase the administrative burden for both regulators and companies, and over time cause regulators to become insensitive to truly harmful data breaches.	We recommend the following: 1. Define what constitutes a "personal information leak." 2. Limit the scope of data breaches requiring notification only to incidents which have the potential to seriously impact or cause serious damages on the affected individuals. 3. Provide a reasonable timeline for a personal information processor to report a data breach. The timeline should start when a personal information processor becomes

	1. The cause of the personal information leak; 2. The categories of leaked personal information and the harm that may be created; 3. Adopted remedial measures; 4. Measures individuals may adopt to mitigate harm; 5. Contact method of the personal information handler. Where personal information handlers adopt measures that are able to effectively avoid harm created by information leaks, personal information handlers are permitted to		aware of such a data incident and allow up to 45 or 60 days for the personal information processor to investigate and assess the data breach before notifying the regulator or the affected individuals.

	not notify individuals; however, where departments fulfilling personal information protection duties and responsibilities believe a personal information leak may create harm to individuals, they may require personal information handlers to notify individuals.		
56	The State cybersecurity and informatization department is responsible for comprehensive planning and coordination of personal information protection work and related supervision and management work. Relevant State Council departments are responsible for personal	It is unclear which regulator companies are to engage as it appears that various parties have enforcement powers. This will increase a personal information processor's compliance cost, such as making it unclear which regulator a data breach shall be reported to, and which regulator designated personal information managers should be registered with.	We recommend clearly listing which regulators will be responsible for what enforcement responsibilities in order to avoid confusion and overlapping reporting requirements.

	information protection, supervision, and management work within their respective scope of duties and responsibilities, according to the provisions of this Law and relevant laws and administrative regulations. County-level and higher People's Governments' relevant departments' personal information protection, supervision and management duties and responsibilities are determined according to relevant State regulations. Departments provided in the previous two Paragraphs are jointly named departments fulfilling personal information protection duties and responsibilities.		

Chapter VII	Legal Liability		
62	Where personal information is handled in violation of this Law or personal information is handled without adopting necessary security protection measures in accordance with regulations, the departments fulfilling personal information protection duties and responsibilities orders correction, confiscate unlawful income, and issue a warning; where correction is refused, a fine of not more than 1 million Yuan is additionally imposed; the directly responsible person	The fines listed in this article seem disproportionate and may discourage companies from processing personal information even when they have a legitimate right to do so. Members report that this phenomenon has already taken place in other jurisdictions that have less severe penalties than those listed in this article. In such cases regulators must then work to convince businesses that: 1. Enforcement of these laws will not target legitimate processing activities, as potential economic growth is lost due to company hesitance. 2. Conduct data activities within the jurisdiction. (in addition to companies), otherwise it would appear disproportionate.	We recommend clarifying that the fine of "50 million RMB or 5% of annual revenue" only apply to a company's China operations and in circumstances where egregious criminal conduct is involved. We also recommend clarifying the specific circumstances in which an individual will be subject to the fines outline in this article.

	in charge and other directly responsible personnel are fined between 10,000 and 100,000 Yuan. Where the circumstances of the unlawful acts mentioned in the preceding Paragraph are grave, the departments fulfilling personal information protection duties and responsibilities order correction, confiscate unlawful income, and impose a fine of not more than 50 million Yuan, or 5% of annual revenue. They may also order the suspension of related business activities, cessation of business for rectification, and report to the relevant competent department for cancellation of corresponding		

	professional licenses or cancellation of business permits. The directly responsible person in charge and other directly responsible personnel are fined between 100,000 and 1 million Yuan.		
Chapter VIII	Appendix		
69	The following terms of this Law are defined as follows: 1. "Personal information handler" refers to organizations and individuals that autonomously determine handling purposes, handling	The requirement that anonymized personal information should be impossible to restore is an impractically high standard. Due to the development of technology, it is highly likely that anonymized information may be de-anonymized in the future. Additionally, the concept of "personal information processor" in the Draft seems to correspond with the concept of "data controller" under the GDPR. Similarly the concept of "entrusted party" in the Draft corresponds to the concept of "data processor" under the GDPR. The lack of shared	We suggest removing "impossible to restore" from the definition of anonymization. We also recommend adopting the replacing the terms "personal information processor" and "entrusted party" with "data controller" and "data processor" respectively to ensure interoperability with global laws and regulations.

	methods, and other such personal information handling matters. 2. "Automated decision making" refers to activities that use personal information to automatically analyze, assess, and decide, via computer programs, individual behaviors and habits, interests and hobbies, or situations relating to finance, health, or credit status. 3. "De-identification" refers to the process of personal information undergoing handling to ensure it is impossible to identify specific	terminology for these concepts may cause confusion when a company drafts an agreement (e.g. a cross-border data transfer agreement making references to these terms under both China and EU legislations).	

	natural persons without support of additional information. 4. "Anonymization" refers to the process of personal information undergoing handling to make it impossible to distinguish specific natural persons and impossible to restore.		