MORRISON | FOERSTER

250 WEST 55TH STREET
NEW YORK, NY 10019-9601

TELEPHONE: 212.468.8000
FACSIMILE: 212.468.7900

WWW.MOFO.COM

MORRISON & FOERSTER LLP

BEIJING, BERLIN, BRUSSELS,
DENVER, HONG KONG, LONDON,
LOS ANGELES, NEW YORK,
NORTHERN VIRGINIA, PALO ALTO,
SAN DIEGO, SAN FRANCISCO, SHANGH
SINGAPORE, TOKYO, WASHINGTON, D.

November 19, 2020

Writer's Direct Contact
+1 (212) 506.7213
MWugmeister@mofo.com

GLOBAL PRIVACY ALLIANCE
COMMENTS ON THE DRAFT LAW OF THE PEOPLE'S REPUBLIC OF CHINA ON THE PROTECTION OF PERSONAL INFORMATION

The Esteemed Legislative Affairs Commission of the Standing Committee of the National People's Congress,

We write on behalf of the Global Privacy Alliance (GPA). We welcome the opportunity to submit comments in connection with the draft Law of the People's Republic of China on the Protection of Personal Information ("draft Law").

The GPA is comprised of a cross section of global businesses from the aerospace, communications, computer and computer software, consumer products, electronic commerce, financial services, logistics, pharmaceutical, professional services and travel/tourism sectors. The GPA works to encourage responsible global privacy practices that enhance consumer trust as well as preserve the free flow of information. Members of the GPA take their privacy obligations very seriously. The views expressed herein generally represent the views of the members of the GPA. While all members support the overall approach presented in this paper, some of the individual points raised may not be relevant to all members.

We enclose our recommendations with respect to the draft Law for your consideration. Should you have any questions or comments, please do not hesitate to contact Miriam Wugmeister, Co-chair of Morrison & Foerster's Global Privacy and Data Security Group in New York, by email at MWugmeister@mofo.com. For your convenience, you may also contact Dan Xuezi in our Beijing office by telephone (010) 5909 3399. Thank you!

Best regards,

Morrison & Foerster LLP

RECOMMENDATIONS

1. Application to Processing Activities Outside of China (Chapter I, Article 3)

Article 3 provides that the Law applies to processing of personal data of natural persons in China that is undertaken outside of China if such activities are conducted to "analyze and assess the behavior of natural persons within the territory". We recommend that this provision be clarified to state the Law applies to processing of personal data of natural persons in China that is undertaken outside of China when such processing activities are related to "the monitoring of behavior of natural persons as far as their behavior takes place inside the borders of China." This change would help to clarify and make this provision consistent with the corresponding provision in the European Union's General Data Protection Regulation ("GDPR").

2. Legal Bases for Processing Personal Information and Sensitive Personal Information (Chapter II, Section 1, Article 13 and Section 2, Article 30)

Article 13 of the draft Law provides for five legal bases for processing personal information, including:

- processing to which the individual has consented ("consent");
- processing that is necessary to conclude or perform a contract with the individual ("contractual necessity");
- processing that is necessary to perform a statutory duty or obligation ("legal requirement");
- processing that is necessary to protect the life, health, or safety of the individual in an emergency ("vital interests"); and
- processing that is carried out for news reporting, public opinion supervision and other activities for the public interest ("public interest").

The trend in data protection law, as evidenced by the GDPR provisions or data privacy laws in Brazil and the Philippines, is to provide a variety of legal bases for processing personal information for uses of data that individuals would reasonably expect to occur. The purpose is to reduce the need to rely on consent as a legal basis for processing. Many jurisdictions have concluded that relying on consent adds a substantial burden on organizations without adding to individuals' privacy protections.

To address this issue, most jurisdictions permit organizations to process personal information for purposes of the legitimate interests pursued by the organization handling the personal information, except where such interests are overridden by the interests or

fundamental rights and freedoms of the individual, and in particular, where the individual is a minor. This would include, for example, cases where

- the personal information is provided to an organization by an individual to enable the organization to provide a service to that individual;
- the personal information is collected by the individual's employer and the collection is reasonable for the purpose of managing or terminating an employment relationship between the organization and the individual;
- transmitting personal information within the group of companies for internal administrative purposes, including the processing of clients' or employees' personal information;
- the processing is necessary and proportionate for the purposes of ensuring network and information security;
- the processing of personal data is necessary for the purposes of fraud prevention, due diligence to fight bribery, and anti-money laundering activities;
- the processing is necessary to exchange business contact information for administration of services (e.g., billing and support);
- the processing of personal information for the organization's own direct marketing purposes.

In addition, most laws provide for additional legal bases such as:

- Processing of personal information that is contained in publicly available sources;
- Processing personal information where the information is subject to a prior dissociation procedure (such as key-coding);
- Processing is necessary for information security purposes (including the use of monitoring technologies in the workplace for network and information security purposes, such as Data Loss Prevention); and
- Processing is necessary to conduct internal investigations into suspected wrongdoings, enforcing internal company policies.

Similarly, processing of sensitive personal information, under Article 30, should be permitted without the individual's consent where necessary for employment purposes. For example, employers often need to process sensitive personal information such as financial data, selected health data, and official identifiers for payroll purposes and provision of benefits such as insurance.

The Law should also provide an exemption for processing of personal information and sensitive personal information for research/historical/statistical purposes. Research purposes should include all types of scientific research, such as clinical research trials. Examples of exemptions that cover research more broadly can be found in many laws such as:

- The GDPR (Article 89) applies to processing of sensitive data for scientific or historical research purposes or statistical purposes;
- Canadian law (Section 7(2)(c) of PIPEDA) applies to statistical, scholarly study or research purposes;
- Malaysia's Personal Data Protection Act (Section 45(2)(c) applies to processing for statistical and research purposes;
- The laws of the Philippines (Section 5-6, Implementing Rules and Regulations of the Data Privacy Act of 2012; Section 4-6 of the Data Privacy Act of 2012) and Singapore (Schedules 3-4 of the Personal Data Protection Act) apply to processing for research purposes.

Some of these additional legal bases are listed in Section 5.6 of China's Personal Information Security Specifications (GB/T 35273—2020). For consistency and clarity, we recommend the Chinese government to consider expanding Articles 13 and 30 to include these additional legal bases for processing personal information and sensitive personal information.

Lastly, we recommend that the Chinese government clarify the contractual necessity legal basis to indicate that it applies to processing that is necessary for the conclusion or performance of a contract to which the individual concerned is a party, *including the implementation of pre-contractual measures or other steps taken at the request of the individual prior to the conclusion of a contract*.

3. Consent (Chapter II, Section 1, Article 14)

Consent should be knowing and voluntary; however, the Law should make clear that such consent can be expressed in different ways, e.g., by providing implicit or explicit consent or authorization. Implicit consent is expressed through actions. For example, when an individual hands out a business card, he or she expects the recipient to use the personal information found on the card to initiate future contacts. Similarly, when an individual contacts an organization to request information and provides mailing contact information, the individual is providing implicit consent to the organization to use his or her personal information to send information. Implicit consent also is considered to be given if the individual, when provided with a clear opportunity to object or opt out of proposed uses of his or her personal information, does not raise objections to such proposed uses. In contrast, explicit or opt-in consent involves express authorization from the individual in verbal, written, or electronic form.

The degree of control permitted and/or the manner in which it may be expressed should depend on the type of information being collected, its intended uses, and/or disclosures.

For example, where sensitive personal data are to be processed on the basis of consent, such consent should be explicit because its misuse would cause serious harm to the individual. Express consent would also be appropriate if the information is to be used for purposes incompatible with the original purposes of collection and use.

Instituting an express consent regime across the board in order to maximize individual control may not be feasible, practical and/or provide any meaningful choices to the individual.

4. Requirements for the Use of Sub-Processors (Chapter II, Section 1, Article 22)

Article 22 requires "entrusted parties" (agents or entities processing under instructions) to obtain consent from the personal information processor before it engages a sub- contractor to carry out processing activities on its behalf. Instead of imposing this consent requirement which would be very burdensome, particularly for companies that engage hundreds or thousands of contractors, we recommend that this provision be revised to mirror the provisions in the GDPR. In particular, the GDPR allows a general written authorization for the use of sub-processors, provided that the agent informs its client of any changes so that the client can object to the use of a sub-processor.

It would also be very burdensome to be required to supervise all entrusted parties. Most companies utilize many suppliers that are independent entities. A more feasible practice would be to require a personal information processor conduct due diligence on a supplier prior to engagement to ensure the supplier has robust privacy policies and compliance measures in place, coupled with strong data protection contractual requirements that would lead to a supplier's liability if breached. If there was evidence of breach of any contractual provisions, a personal data handler could then inspect and audit a supplier.

5. Disclosures to Third Parties (Chapter II, Section 1, Article 24)

Article 24 requires a personal information processor that provides any personal information to a third party to inform the individuals concerned of the third party's identity and contact information, the purpose and method of processing, and the types of personal information, and obtain a separate consent of the individuals concerned.

Article 24 does not specify if this requirement applies to all third parties (other personal information processors and agents/service providers). If this provision is intended to apply to agents/service providers, we would like to highlight the following concerns;

- We believe that imposing a requirement to identify third party agents/service providers by name rather than simply specify the categories of recipients raises serious security concerns and does not substantially enhance the privacy protections afforded to individuals. Companies often use service providers as a way of providing better security for their data. Part of the assessment involves using a variety of service providers so that all of the company's most important data are not all in one place. Making public the identity of the recipients would give bad actors information on where exactly to find an organizations' data and a road map of the vendors that are likely to have the most valuable data. Moreover, multinational companies engage hundreds of service providers for varying periods of time. Their list of service providers is constantly changing. Requiring companies to notify individuals regarding the identity of all of their service providers imposes an enormous administrative burden and does little to enhance individuals' privacy rights. In addition, the trend now is in favor of having notices that are short and easy to understand. Listing each and every service provider is contrary to that goal.
- If disclosures to a service provider are necessary in order to provide a product or service requested by the individual or if third party entities have been hired by the organization to perform services on its behalf, then it is unreasonable to require consent from affected individuals, provided that the organization agrees to remain accountable for the handling of the information by its agents and service providers. When the information involved is such that its misuse is likely to result in significant harm to the individual, it is reasonable to require organizations and their agents to take proper steps to protect the information against such misuse. Imposing appropriate security or special handling requirements will afford greater protection to the individual than simply requiring consent. If the individual wants the product or service, then there is little real choice in the matter and relying on consent simply shifts the burden from the organization to the individual. Requiring consent does not in fact enhance the privacy protections of the individuals.

We recommend, therefore, that Article 24 be revised to clarify that the provisions pertains to third party personal information processors (i.e., controllers under GDPR) only.

6. Definition of Sensitive Personal Information (Chapter II, Section 2, Article 29)

To make this Law consistent with many privacy laws around the world, we recommend that the Chinese government exclude financial account information from the definition of sensitive personal data. Moreover, financial information is often regulated under the laws specific to financial institutions. Financial information can cover a wide array of information (e.g., bank name, account or credit card number, account password). Individually, these

data are not sensitive per se; however, a combination of these data (e.g., account, password and name) if subject to a data breach could pose a risk to the individual. In such cases, the data breach rules can be used to trigger the appropriate response. Most data protection laws, including the GDPR, do not include financial information in their definition of sensitive personal data.

7. Rules for Cross-border Provision of Personal Information (Chapter III, Articles 38-39)

Under Article 38, a personal information processor must satisfy one of the following conditions in order to transfer personal information to recipients outside of China:

- pass the security assessment conducted by the cyberspace administration department of the State in accordance with Article 40 of this law;
- be certified by a specialized agency in accordance with the requirements of the cyberspace administration department of the State;
- conclude a contract with the overseas recipient that establishes the rights and obligations of both parties, and enables the personal information processor to supervise the processing activities to ensure they meet the personal information protection standards specified in this law; or
- meet the other conditions prescribed by laws, administrative regulations or the cyberspace administration department of the State.

Article 39 further requires the personal information processor to notify the individual concerned of the identity and contact information of the overseas recipient, the purpose and method of processing, the types of personal information, as well as the method for the individual to exercise his or her rights hereunder against the overseas recipient, *and obtain the individual's separate consent*.

Imposing a consent requirement in addition to satisfying one of the Article 38 conditions is overly burdensome and does not enhance protection of personal information in a meaningful way. There are a number of problems with using a consent approach for cross-border transfers. First, requiring individuals to consent to the cross-border transfer of their personal information, particularly on top of the consent they may have to provide at the time collection will lead to consent "fatigue" (e.g., individuals simply click yes without reading or understanding the underlying information). Anecdotal evidence as well as a number of studies have found that individuals do not read privacy policies or are willing to overlook invasive activity if the service being offered is something that they desire.

Second, there are a number of situations in which individuals do not truly have choice and thus basing cross-border transfers on consent is meaningless or will lead to negative

outcomes for individuals and organizations. For example, if a company wishes to use a service provider overseas to process payroll and consent from the employee is required, will the employee really have the ability to say "no" – what will be the ramifications if the individual says no? Will the employer have the ability to take the position that consent is a condition of employment and the failure to consent will be that the employee loses his/her job? Or will the company have to set up a second payroll system for that individual and thus spend twice as much money to perform a basic function because one employees refuses to consent to payroll being processed overseas? Or will the company not be able to use the payroll vendor it deems the best because a single employee refuses to consent? All of those options are problematic and suggest that consent in that context is not a viable solution.

Third, individuals are not generally in the best position to determine if the receiving company should be provided with the information or whether the protections they have promised will be sufficient. Even with the most transparent privacy policy, individuals often are not able to determine if the security promises a company makes are sufficient, or if the proposed uses of personal information are reasonable. Those are complicated and nuanced judgements and individuals may not have the skills or interest to determine if the disclosures provided by an organization should give them pause. Requiring consent, simply moves the responsibility from the company to the individual. Thus a company that wishes to use a service provider is in the best position, not the individual, to evaluate and impose obligations on the service provider.

There are also other problems with this approach from the business perspective. Requiring a separate consent for cross-border transfers, beyond the consent that must be obtained to collect and process the information for specified purposes, adds time and expense. Because individuals will be able to withdraw their consent, the business's service provider relationships may be disrupted at any time. For example, imagine that an organization elects to use a company in Ireland to handle its call center operations. The organization signs a contract and sets up the call center. Now suppose that a consumer who is entitled to customer service objects to having his information sent to Ireland. Will the organization need to provide an alternative way to provide the call center services in China because a single consumer does not consent or will the Chinese company be put in the position of breaching its promises to the consumers and tell the individual that he is not entitled to customer service if he does not consent to the information being in Ireland? Both results are untenable.

Similarly, in the employment context, if a company choses to use a cloud service vendor to store HR data and an employee changes her mind and withdraws consent for the transfer of the data, will the company need to bring all of the HR data hosting back in house at the cost

of tens of millions of RMB or will the company be permitted to terminate any employee who does not agree to having the HR data stored in the cloud service?

Another example relates to the need to share information to defend legal claims or to cooperate with an investigation with a foreign regulator. Suppose an organization in China is required to share information in the context of a litigation in another country or is requested to share information with a government authority because of an ongoing investigation. What will happen if a consumer refuses to consent to sharing information with the foreign court or the foreign regulator? The Chinese company will find itself having to pick which law to violate (the Chinese Law or the obligation to a non-Chinese court or regulator). That seems to put organizations in a very difficult position.

For these reasons we recommend the Chinese government to eliminate the separate consent requirement for cross border transfer of data. Many countries such as the EU member states, Australia, Brazil, and Singapore permit organization to transfer personal information cross-border either on the basis of a contract or consent – but not both. Consent can be one alternative as it is in these countries but there should be ways for Chinese companies to share information cross border without obtaining the consent of the individual. For example, in the EU, controllers or processors may transfer personal information outside the EU where they have provided appropriate safeguards such as through EU Standard Contractual Clauses. In such cases, individuals do not need to give their consent to the transfer. Similarly, Singapore permits such transfers without the need for consent where there is a contract in place that requires the recipient outside of Singapore to provide a standard of protection for the transferred personal data that is at least comparable to the protection under the Singapore law.

8. <u>Data Localization</u> (Chapter III, Article 40)

We recommend the Chinese government to limit the data localization requirements to critical information infrastructure operators only or to issues that implicate national security. Expanding such requirements to apply to other types of personal information processors will have a negative impact on businesses that rely on cross-border data transfers to provide services to customers in China and disrupts the provision of such services. Data localization would reduce the ease of doing business in China, because data-reliant companies would not be able to transfer data easily to affiliated companies or business partners or service providers outside China. Data localization requirements would also adversely impact the competitiveness of Chinese companies that provide services which are reliant on cross-border data transfers.

Data localization requirements and cross-border data restrictions will have significant and unintended consequences for domestic economic growth and investment. Every sector of

the economy, be it manufacturing, services, agriculture, or retail, depends on global data flows. Data flows make markets more efficient by reducing the barriers of entry into new and distant markets, particularly for individuals, start-ups and small-to-medium enterprises. In addition, such flows reduce transaction costs, increase organizational efficiencies, accelerate the spread of ideas, and enable businesses to make use of new research and technologies.[1]

9. Local Data Protection Officer ("DPO")/Specialized Department (Chapter III, Article 52)

Article 52 requires a personal information processor outside of China to establish a specialized agency or designate a representative within China to be responsible for personal information protection matters, and report the name and contact information of the relevant agency or representative to the department performing personal information protection duties. We recommend the Chinese government to consider a more flexible approach – one that would enable the personal information processor located outside of China to select its DPO or specialized department based on qualifications and organizational structure rather than physical location. For example, under the GDPR, one DPO (or specialized department) can be designated for a group of undertakings, provided that the DPO (or specialized department) is "easily accessible from each establishment". This means that individuals, the relevant data protection authorities, and the employees within each covered organization must be able to reach the DPO (or specialized department) easily, directly, and confidentially without having to contact another part of the organization. The European Data Protection Board acknowledges that where the organization has no establishment within the EU, a DPO (or specialized department) may be able to carry out its activities more effectively if located outside the EU.

6. Personal Data Breach (Chapter III, Article 55)

Breach notification obligations can serve important individual and public policy objectives. From the individual perspective, the primary purpose of notification is to enable individuals to mitigate the risk of identity theft or fraud when a breach occurs. In contrast, the primary purpose of government reporting is to enable the authorities to exercise their regulatory oversight functions, for example, to identify persistent or systemic security problems and take action as needed to address those problems and to assist individuals who may be harmed by a breach. In addition, individual and public authority reporting obligations can serve to motivate organizations to implement more effective security measures to protect

[1] See Deloitte's 2014 report on Value of connectivity – Economic and social benefits or expanding internet access, available at https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/TechnologyMediaCommunications/2014_uk_tmt_value_of_connectivity_deloitte_ireland.pdf.

sensitive information. Therefore, because notification to individuals and public authorities serves different purposes, there should be different notification triggers for both groups.

Moreover, the goal of breach notification provisions should be to define a reasonable and balanced notification trigger that ensures that individuals receive notice when there is a significant risk of substantial harm as a result of a security breach but that does not result in over-notifying and desensitizing individuals to these important notices.

When imposing notification obligations, the Law or implementing regulations should specify the personal information that would be subject to these obligations. Specifically, notification should be based on the types of information that could be used to cause the "significant harm" that the notification requirement is designed to help individuals mitigate.

With respect to a risk of identity theft or financial fraud, the notification obligation should be limited to identifiable and unencrypted data that includes one or more sensitive data elements, such as a national identification number (or other number that can be used to open a financial account) or financial account information together with any password or pin number that can be used to access the underlying account. With respect to a risk of substantial harm from the misuse of health information, the notification obligation should be limited to identifiable and unencrypted data that include an individual's name together with one or more sensitive health data elements, such as a national identification number or health information, such as, for example, a medical diagnosis ("Specified Personal Information").

Lastly, it would be helpful to clarify that a personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.