HAN KUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

Han Kun Newsletter

Issue 183 (7th edition of 2022)

Legal Updates

1. CAC Formally Promulgates the Assessment Measures for Data Export
2. A Brief Look at China Draft SCC for Personal Information Export

1. CAC Formally Promulgates the Assessment Measures for Data Export

Author: Kevin DUAN | Kemeng CAI | Tina WANG | Zihuan XU | Jin JIN

On July 7, 2022, the Cyberspace Administration of China (the "**CAC**") formally promulgated the *Measures for Security Assessment of Cross-border Data Transfers* (the "**Assessment Measures**"), which specify and implement the provisions on data export in accordance with Article 37 of the *Cybersecurity Law of the People's Republic of China* (the "**CSL**"), Article 31 of the *Data Security Law of the People's Republic of China* (the "**DSL**"), and Articles 36, 38, and 40 of the *Personal Information Protection Law of the People's Republic of China* (the "**PIPL**"). The Assessment Measures generally continue with strict supervision toward data exports and adopt the institutional framework proposed in the *Measures for Security Assessment of Cross-border Data Transfers (Draft for Comment)* (the "**Draft Assessment Measures**"), issued by the CAC on October 29, 2021, but relaxed provisions are also found in their details. In this newsletter, we briefly analyze the main contents of the Assessment Measures and highlight notable key issues and potential challenges.

Defining the "export of personal information and important data"

According to Article 2 of the Assessment Measures, applicable data export activities are those where data handlers provide cross-border important data and personal information collected and generated in the course of their operations within China mainland. In addition, the export of de-identified personal information also falls into the application scope of the Assessment Measures in accordance with the definition of personal information stipulated in Article 4 of the PIPL.

As for understanding the "export of personal information and important data", we summarize the applicable data export activities under the Assessment Measures into two categories in line with the introduction of CAC's accompanying press briefing[1], which include: (i) cross-border transfer and storage of data collected and generated in China mainland; and (ii) storing data collected and generated in China mainland, but providing overseas institutions, organizations, and individuals with right of access and use to such data.

In addition, significant concerns have been raised as to whether the Assessment Measures apply to the circumstances stipulated by Article 3.2 of the PIPL i.e., whether overseas entities' direct collection of personal information from domestic personal information subjects is subject to a cross-border data transfer security assessment ("**Security Assessment**"). The Assessment Measures do not clearly address this issue, and it needs to be further clarified in subsequent supervision practice. However, considering the system interpretation, we tend to take the view that, for personal information, "export" in the Assessment Measures only refers to circumstances where domestic personal information handlers export personal information in accordance with Chapter III of the PIPL. In other words, an overseas entity may not be required to perform a security assessment under the Assessment Measures to directly collect personal information from domestic personal information subjects. In view of the uncertainty in the application

[1] CAC's accompanying press briefing published on July 7, 2022, for more details please refer to: http://www.cac.gov.cn/2022-07/07/c_1658811536800962.htm (last access on July 8, 2022).

scope of the Assessment Measures, it is advisable for relevant enterprises to pay close attention to regulatory developments and to consider obtaining a personal information protection certification when collecting personal information directly from domestic personal information subjects, in accordance with the *Practice Guidelines for Cybersecurity Standards - Technical Specifications for the Certification of Personal Information Cross-border Processing,* officially issued by the Secretariat of the National Information Security Standardization Technical Committee on June 24, 2022.

Circumstances subject to the application for Security Assessment

Article 4 of the Assessment Measures specifies four circumstances subject to the Security Assessment, which are:

- data handlers who export important data;
- critical information infrastructure operators or personal information handlers who export personal information and have processed the personal information of at least 1 million individuals;
- data handlers who have cumulatively exported personal information of at least 100,000 individuals or sensitive personal information of at least 10,000 individuals since January 1 of the previous year;
- other circumstances where an application for Security Assessment is required as prescribed by the CAC.

The following are key points for these applicable circumstances.

I. All exports of important data are subject to the Security Assessment[2]

According to Article 31 of the DSL, the CAC is entitled to formulate regulations for the export of important data. Accordingly, Article 4 of the Assessment Measures requires all circumstances where data handlers export important data to be subject to an application for Security Assessment, which indeed broadens the application scope of Security Assessment with respect to important data exports stipulated by Article 37 of the CSL.

II. The thresholds for determining personal information exports is limited to a maximum of two years

Overall, the Assessment Measures follow the cumulative thresholds proposed by the Draft Assessment

[2] According to Article 19 of the Assessment Measures, important data are those data that once tampered with, destroyed, leaked, illegally obtained or illegally used, may endanger national security, economic operation, social stability, public health and safety, etc. The Assessment Measures do not clearly list specific types of important data, so the identification of important data still needs to be clarified in accordance with other laws, regulations and standards. Based on the DSL each region or department is responsible for formulating a specific catalog of important data in its own region, department, and relevant industries and fields. The National Information Security Standardization Technical Committee has begun to formulate relevant national standards since 2020, and the *Information security technology - Guideline for identification of critical data (Draft for Comments)* has been reviewed and revised for several rounds as of January 7, 2021, which will provide principal guidance for the formulation of specific catalogs of important data in each region and department. Among industry regulations, the *Several Provisions on Automotive Data Security Management (Trial Implementation)* applied to the automotive industry define important data (involved in the process of automobile design, production, sales, use, operation and maintenance) as the data that, once tampered with, destroyed, leaked or illegally obtained or illegally used, may endanger national security, public interest or the legitimate rights and interests of individuals and organizations, and list the specific types of such important data.

Measures for determining the quantities of personal information processed or exported. However, the export thresholds for personal information of 100,000 individuals and sensitive personal information of 10,000 individuals are considered on a rolling basis from January 1 of the previous year. In other words, the thresholds are determined over a maximum period of two years and these quantities are not accounted for on a perpetual basis. This will reduce compliance costs for small businesses whose quantities of personal information exported are relatively small.

Relationship between local storage and the Security Assessment

Controversy exists as to whether enterprises are required to localize their personal information in China under Article 40 of the PIPL if they meet one of the thresholds for processing or exporting personal information under the Assessment Measures. We take the view that although the Assessment Measures do not explicitly mention a localization requirement, Article 40 of the PIPL expressly stipulates that "critical information infrastructure operators" or "personal information handlers who process personal information meet the threshold prescribed by the CAC" are required to perform two data export obligations, namely "local storage" of personal information collected and generated in China and passing a "Security Assessment" when it is indeed necessary to export such data. Therefore, theoretically, localization is in essence a mandatory obligation of enterprises that meet the quantity threshold prior to export. In addition, local storage also helps competent authorities to carry out more efficient supervision of data security. However, considering the low quantity threshold set by the Assessment Measures, it remains to be seen in practice whether the competent authorities will strictly require "local storage" to pass the Security Assessment. Because the lengthy process of the Security Assessment and the uncertainty of its results, data localization (i.e., local storage and avoidance of data exports) may become an option forced upon many enterprises.

Self-Assessment as a precursor

As for the cross-border data transfer risk self-assessment requirement (the "**Self-Assessment**"), Article 5 of the Assessment Measures stipulates that "data handlers shall carry out [Self-Assessments] before applying for the [Security Assessment]". The matters to be assessed include the legality, legitimacy and necessity of the export as well as the purpose, scope, and method of the data processing of overseas receivers; the quantity, scope, type, sensitivity and risk of data exported; the protection capabilities of overseas receivers; security risks during and after data cross-border transfer and the protection of personal information rights and interests; and contractual arrangements governing the responsibilities and obligations of both parties for data security and protection in contracts or other legally binding documents drawn up for the data export (collectively, "**Legal Documents**"). As for personal information exports, a similar internal assessment requirement is also stipulated in Article 55 of the PIPL and the *Provisions on the Standard Contract for the Export of Personal Information (Draft for Comment)* (the "**Draft Provisions**"), both of which require data handlers to carry out a personal information protection impact assessment before exporting personal information. In practice, we take the view that enterprises may integrate internal assessment processes. That is, enterprises may first carry out a personal information protection impact assessment, and on such basis complete the Self-Assessment in accordance with the Assessment Measures. In general, regardless of whether the enterprise is a critical infrastructure operator or meets

a quantity threshold related to personal information, a prior internal assessment is a necessary compliance requirement that must be fulfilled before exporting personal information and important data.

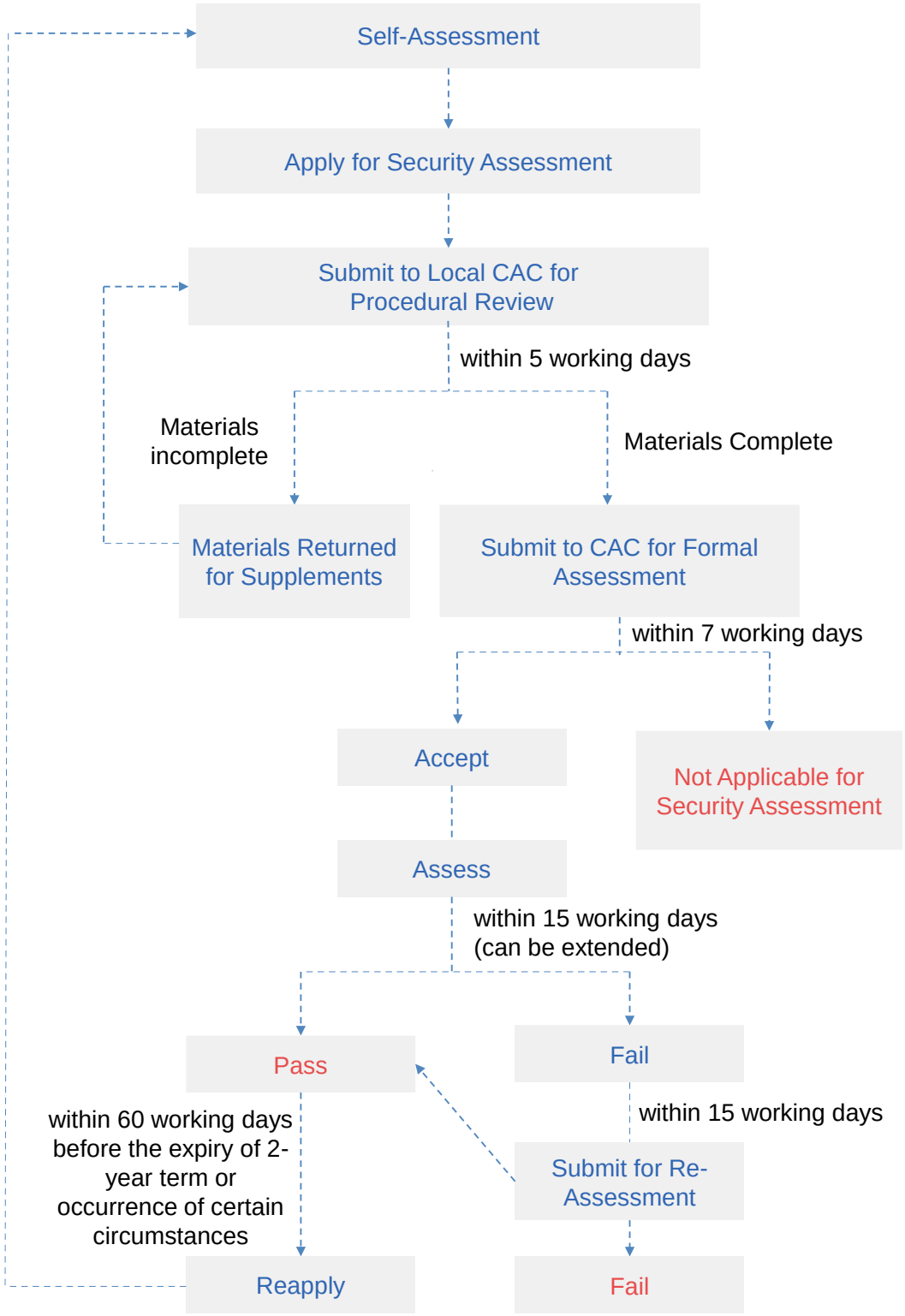
Draw up data export legal documents before applying for the Security Assessment

Data handlers will be required to submit Legal Documents for data export drawn up with overseas receivers when applying for the Security Assessment. According to Article 9 of the Assessment Measures, the Legal Documents include the following terms: the purpose, method and scope of data export; the processing of overseas receivers; the status of data stored overseas; binding clauses restricting the transfer of the exported data by overseas receivers to other organizations and individuals; the security measures that the overseas receiver should take when the actual control or business scope of overseas receivers undergo a substantial change, the data security protection policies and regulations and the cybersecurity environment of the country and region where it is located; changes or other situations caused by force majeure occur; remedies and liabilities for breaches of data security protection obligations and dispute resolutions; and emergency response requirements and channels for individuals to safeguard their exercise of personal information rights.

The Draft Provisions, together with the *Draft Standard Contract for the Export of Personal Information*, could serve as references for the template contract (for the export of personal information) or important references (for the export of important data). Apart from contracts, other legally binding documents may include unilateral commitment letters from overseas receivers or the data security management systems or policies formulated by corporate groups of domestic data providers and overseas receivers. However, as CAC's accompanying press briefing introduces, data handlers should not formally sign the Legal Documents with their overseas receivers until they pass the Security Assessment; otherwise, they should instead make contractual arrangements that condition the effectiveness of such Legal Documents on passing the Security Assessment.

Rigorous procedures of the Security Assessment

According to Articles 7 and 11-14 of the Assessment Measures, detailed procedures for the Security Assessment are illustrated by the following diagram:



Key points of the aforesaid procedures are as follows:

I. Procedural review by the local CAC

Compared to the Draft Assessment Measures, Article 7 of the Assessment Measures adds a procedure for the CAC at the provincial level to undertake a preliminary review of the completeness of application materials within five working days of the date of receipt. After this procedural review, the provincial-

level CAC will submit the application materials to the CAC, unless it requires the data handler to supplement its application materials if they are found to be incomplete.

II. Removal of the maximum extension period for the Security Assessment

Notably, Article 12 of the Assessment Measures removes the 60-working-day maximum extension period for the Security Assessment stipulated by Article 11 of the Draft Assessment Measures. According to Article 12 of the Assessment Measures, the CAC may extend the assessment for an appropriate period and notify the data handler accordingly, where it finds the case is complicated or there are materials to be further supplemented or corrected. However, there is no explicit limit for this "appropriate period". Therefore, while the assessment period is generally 45 working days, it may be further extended to more than 60 working days. In practice, the data processing activities of enterprises are usually time-sensitive and continuous, so a lengthy assessment period may bring greater uncertainty to the export of various customer data and employee data related to enterprises' operations.

III. Three outcomes of the Security Assessment

There are three possible outcomes of the Security Assessment. First, the Security Assessment is not applicable, in which case the CAC will notify the data handler within seven working days of receiving the application materials that the data export is not subject to the Assessment Measures. In other words, the data handler could then carry out its data export through other lawful means. Second, the data handler passes the Security Assessment, in which case the data handler will be allowed to carry out the data exports upon receiving written notice and strictly in accordance with its application. Third, the data handler fails the Security Assessment, in which case the data handler is prohibited to conduct the data export and must revise its data export plan (such revisions may include reducing the scope or frequency of data export or enhancing the security protection measures after data export) and then reapply for the Security Assessment or adopt data localization measures to avoid exporting the data.

IV. Supplementing procedures for objection and re-assessment

Article 13 of the Assessment Measures adds a procedure for objection and re-assessment on the basis of the Draft Assessment Measures. A data handler who has an objection to the assessment results may apply for a re-assessment to the CAC within 15 working days of the date of receipt of the assessment result; the result of the re-assessment is final. This new procedure provides an additional remedy for enterprises that fail an initial Security Assessment.

Focus of the Security Assessment

Overall, according to the Assessment Measures, the focus of CAC when conducting the Security Assessment is consistent with that stipulated under the Draft Security Measures. The key points are as follows.

- **Understanding the necessity of the data export:** compared with cross-border data transfers, the alternative choice for data localization usually results in a significant increase in operating cost and great inconvenience; for example, it may be hard for international collaborations on certain

tasks and the use of different IT providers may lead to the inability to interconnect, etc. However, whether such considerations could contribute to the necessity of a data export is controversial in practice.

- **Assessing the impacts of security protection policies and regulations and cybersecurity environment of the country or region where the overseas receiver is located on the security of exported data:** conclusions of the following topics need to be further explored and examined in practice—whether the CAC will make adequacy decisions similar to foreign data protection authorities on the data protection level in a specific country or region; whether the CAC will entrust third-party monitoring agencies or academic institutions to make assessment reports; in particular, in the context of intensified global geopolitical and trade conflicts, whether the restrictions on cross-border data transfer to China or other restrictive measures imposed by other countries or regions will affect the results of a Security Assessment.

Continuous assessment and supervision

The Security Assessment is not a one-time assessment. The Assessment Measures aim to establish a continuous assessment and supervision mechanism by which data handlers can normally carry out data export activities during the two-year validity period of the Security Assessment results. However, if one of the prescribed circumstances occurs during the validity period, or if the validity period of the result expires, the data handler will be required to re-apply for a Security Assessment.

Specifically, after a data handler has passed the Security Assessment conducted by the CAC, it is not required to re-apply during the two-year period for subsequent or successive transmissions of similar data to the same receiver. However, data handlers will be required to re-apply for a Security Assessment in the following circumstances (Articles 14, 17):

- where the purpose, method, scope, and type of data provided overseas, and the use and method of data processing by overseas receivers have changed, or the overseas retention period of personal information and important data has been extended;
- where the data security protection policies and regulations and the cybersecurity environment of the country and region where the overseas receiver is located have changed, or other situations caused by force majeure have occurred, the actual control of the data handler or the overseas receiver has changed, or changes in the Legal Documents between the data handler and the overseas receiver, etc. may affect the security of the data export;
- other circumstances that may affect the security of the data exported;
- where the CAC finds the data export activity that passed a Security Assessment no longer meets the data export security management requirements in actual processing.

Cure period

The Assessment Measures will become effective on September 1, 2022 (the "**Effective Date**"). Compared to the Draft Assessment Measures, Article 20 of the Assessment Measures provides a cure

period for data handlers to rectify within six months any non-compliance in existing data export activities carried out before the Effective Date, i.e., before March 1, 2023. Therefore, data export activities subject to the Assessment Measures but carried out before the Effective Date will not be currently affected. However, relevant data handlers should apply for the Security Assessment as soon as possible to ensure relevant ongoing data export activities are in compliance with laws and regulations.

Our comments

The Assessment Measures propose unprecedentedly strict restrictions on the export of important data and certain quantities of personal information from China mainland. Combining the Security Assessment for personal information and important data into one regulation reflects China's caution and concern over the national security risks posed by exporting large amounts of such data. In summary, the Assessment Measures will not only bring structural IT adjustments, internal organizational restructuring, and the consequent huge upfront investment costs to MNCs in China, but will also generate a lot of continuous daily compliance expenses for processes such as examining data exports, data cross-border transmission agreement management, and continuous supervision of the subsequent outbound use of exported data. To address the compliance challenges posed by the Assessment Measures, it is advisable for enterprises to consider the following suggestions.

- **Consider Local Data Storage**: the Assessment Measures set low quantity thresholds for the mandatory Security Assessment; as a result, enterprises whose businesses presently rely on overseas data processing or centralized storage will inevitably need to consider localization as an option to avoid lengthy assessment procedures and the uncertainty that they bring.
- **Improve internal systems and prepare relevant templates**: the Assessment Measures do not set a maximum time limit for the assessment period, which will bring uncertainty and high potential time costs to enterprises' data export activities. Enterprises who intend to carry out data export activities in the future are advised to formulate an internal data export identification system and a self-assessment system and to prepare relevant Legal Documents in advance, which will serve as key components to smoothly promote data export activities.
- **Carry out data mapping, apply for a Security Assessment as early as possible, and complete rectifications within the cure period**: the cure period is six months after the Effective Date. Before the expiration of the cure period, all enterprises subject to the Security Assessment requirement should begin examining their related data export activities as early as possible and prepare to apply for a Security Assessment in order to avoid the circumstance where the data export activities cannot be carried out upon expiration of the cure period.

2. A Brief Look at China Draft SCC for Personal Information Export

Authors: Kevin DUAN | Kemeng CAI | Minzhe HU | Ziqian ZHANG | Yi ZOU

On June 30, 2022, the Cyberspace Administration of China (the "**CAC**") issued the *Provisions on the Standard Contract for the Export of Personal Information (Draft for Comment)* (the "**Draft Provisions**") and the *Draft Standard Contract for the Export of Personal Information* (the "**Standard Contract**"). The Draft Provisions are composed of 13 articles and clarify the Standard Contract's application scope, conditions of application, main contents, etc., aiming to specify the requirements for transferring personal information cross-border by signing standard contracts formulated by CAC authorities under Article 38.3 of the *Personal Information Protection Law* ("**PIPL**"). Notably, the Draft Provisions require personal information handlers to conduct filing procedures with the provincial-level CAC within 10 working days from the effective date of the Standard Contract. Although the filing does not affect the effectiveness of the contract and the export of personal information, the requirement provides the regulatory authorities with useful tools to supervise the export of personal information.

The Standard Contract includes 9 articles and 2 appendixes, focusing on the obligations of personal information handlers, the obligations of the overseas recipients, the rights of personal information subjects, the impact of personal information protection policies and regulations in overseas countries or regions on compliance with the contract terms, remedy measures, contract termination, liability for breach of the contract, governing law and dispute resolution.

We will briefly summarize the main contents of the Draft Provisions and the Standard Contract, and provide practical suggestions for companies to use and implement the Standard Contract in practice.

Application scope of the standard contract

I. Circumstances where personal information may be transferred cross-border under the Standard Contract

Article 4 of the Draft Provisions specifies all four conditions that a personal information handler is required to satisfy when providing personal information cross-border by entering into the Standard Contract, including:

1. Not classified as a critical information infrastructure operator (the "**CIIO**");
2. Processes personal information of less than one million individuals;
3. The cumulative amount of personal information provided cross-border has not reached 100,000 individuals since January 1 of the previous year;
4. The cumulative amount of sensitive personal information provided cross-border has not reached 10,000 individuals since January 1 of the previous year.

The above four conditions exclude the circumstances where personal information handlers are required apply to CAC for a data export security assessment under the PIPL and the *Measures on*

Security Assessment of Data Export, which are expected to be formally issued soon. However, this does not mean that personal information handlers do not need to sign the Standard Contract when applying for a data export security assessment, rather that they may not transfer personal information cross-border solely by executing the Standard Contract. In other words, personal information handlers will need to apply to CAC for a security assessment in addition to executing the Standard Contract.

It should be noted that the quantity standards specified in the above items 2, 3 and 4 are consistent with the *Measures for Security Assessment of Data Export (Draft for Comments)* **("Draft Assessment Measures")** issued in 2021 [3]and will be likely to be adopted in the subsequent finalized version. In addition, items 3 and 4 above clarify the time span standard of "cumulative quantity" which is generally concerned by the personal information handlers, and specify that the quantity of personal information or sensitive personal information provided cross-border will be calculated from January 1st of the last year. We take the view that setting 1-2 years as the cumulative period of personal information quantity, to a certain extent, is beneficial for companies with small scale of personal information to use the Standard Contract, which is a relatively convenient method, to transfer personal information cross-border.

II. The Standard Contract does not appear applicable to overseas entities that directly collect personal information from domestic individuals

The circumstance where overseas entities directly collect personal information from domestic individuals is not similar to the circumstance where domestic personal information handlers provide personal information to overseas recipients and may not be deemed as the "export of personal information" under Article 38 of the PIPL and the Draft Provisions. Therefore, it seems that overseas entities may not rely on the Standard Contract when they directly collect personal information from domestic individuals. However, if the overseas entity is subject to the Article 3.2 of the PIPL, its collection and processing of personal information of domestic individuals will still constitute the "export of personal information", and its specialized agencies or designated representatives in China may apply for certification in accordance with the *Practice Guidelines for Cybersecurity Standards - Technical Specifications for the Certification of Personal Information Cross-border Processing*, and assume relevant responsibilities.

Key terms of the standard contract for the export of personal information

The Standard Contract was issued alongside the Draft Provisions and consists of 9 articles and 2 appendixes, which set out the rights and obligations of the personal information handler and the overseas recipient, respectively, and specify the rights of the personal information subject. In terms of substantive obligations, the Standard Contract is aligned with the latest standard contractual clauses (the "**SCC**") issued by EU regulators in accordance with the GDPR. However, the Standard Contract embodies some original provisions according to the requirements of the PIPL. Predominantly, the Standard Contract does

[3] On July 7, 2022, CAC issued the final version of the Measures on Security Assessment on Data Export **("Measures")** which will come into effect on September 1, 2022. You may refer to our other legal commentaries about this Measures on our website.

not distinguish four modules as provided in the newly published SCC, which separately applies to transfers from controller to controller, transfers from controller to processor, transfers from processor to sub-processor, and transfers from processor to controller. Instead, the Standard Contract distinguishes the overseas recipient as an independent personal information handler from that as an entrusted processor under some provisions and stipulates different requirements.

I. Basic information

The Standard Contract requires that the domestic personal information handler and the overseas recipient clearly record in Appendix I the basic facts of the export of personal information, including (i) the information of the personal information handler and the overseas recipient, such as name, address, contact name, contact information, etc., which are stipulated in the contract as usual; and (ii) basic information of the personal information export, which should be described in Appendix I, including the purpose, scope, type, sensitivity, quantity, method, retention period, retention location, and other aspects of personal information to be transferred cross-border.

II. Obligations of the personal information handler

Article 2 of the Standard Contract specifies the obligations of the personal information handler. Apart from those obligations regarding the export of personal information under relevant laws and regulations, the personal information handler is also responsible for supervising the overseas recipient. The personal information handler will become the regulatory authorities' target in regulatory enforcement actions and the main responsible party for the export of personal information in accordance with Article 2 of the Standard Contract, which sets out the responsibility of the personal information handler, and Article 9.6, which requires personal information handler to indemnify any losses of the personal information subjects. Specifically, the obligations of the personal information handler include:

1. **The principle of minimum necessity:** the personal information to be transferred cross-border must be limited to the minimum extent necessary for the purposes of processing.

2. **Notification:** apart from the requirement stipulated in Article 39 of the PIPL that the personal information subject must be informed of the name of the overseas recipient, contact information, purpose and method of processing, type of personal information and the method and procedure for the individuals to exercise their rights, the Standard Contract also requires the personal information handler to inform the individuals of the information of third parties who receive their personal information in onward transfers, the retention period and the retention location after export, and other relevant information required in Appendix I. In addition, the Standard Contract further stipulates that personal information subjects must be informed that the personal information handler and the overseas recipient have agreed through the Standard Contract that he or she is a third-party beneficiary and he or she is entitled to such rights in accordance with the Standard Contract if he or she does not expressly object within 30 days.

3. **Separate consent:** the Standard Contract requires that the personal information handler obtain separate consent from the personal information subject, but leaves some room for enterprises to transfer personal information cross-border based on a legal basis other than the individual's consent.

4. **Review whether the overseas recipient is in compliance:** the personal information handler must make reasonable efforts to ensure that the overseas recipient has fulfilled its obligations and adopted necessary technical and organizational measures for the personal information to be transferred in consideration of its volume, sensitivity, retention period and retention location.

5. **Provide a copy of the PRC laws and technical standards to the overseas recipient:** upon request of the overseas recipient, the personal information handler must provide the overseas recipient with a copy of the relevant PRC laws and technical standards.

6. **Respond to the regulatory authorities:** in principle, personal information handlers must respond to inquiries from the regulatory authorities, unless both parties agree that the overseas recipient will respond. It should be noted that if the overseas recipient fails to respond within the time limit as required, the personal information handler remains responsible for such inquiry.

7. **Conduct personal information protection impact assessments**: the personal information handler represents that it has conducted a personal information protection impact assessment (please refers to Part III of this Article) and retain the personal information protection impact assessment report for at least three years.

8. **Provide a copy of the Standard Contract to personal information subjects:** the personal information handler is required to provide a copy of the Standard Contract to personal information subjects upon their request. To the extent necessary to protect trade secrets or other confidential information (such as the contents of protected intellectual property rights etc.), relevant contents hereof may be appropriately redacted. Nonetheless, the personal information handler is required to provide personal information subjects with an effective summary to help them understand the contents of the Standard Contract.

9. **Assume the burden of proof:** the personal information handler bears the burden of proving that the obligations stipulated in the Standard Contract have been fulfilled.

10. **Provide to regulatory authorities proof that the overseas recipient is in compliance:** the information referred to in Article 3.10 of the Standard Contract, including all audit results, must be provided to the regulatory authorities as required by applicable laws and regulations. Therefore, the personal information handler is entitled to review relevant data and materials or conduct an audit for the relevant processing activities.

III. Obligations of the overseas recipient

The Standard Contract imposes contractual obligations on the overseas recipient that are intended to provide personal information subjects in China with the same level of protection mandated by the PIPL for their personal information when it is transferred cross-border. In addition, the Standard Contract also stipulates the obligations and responsibilities of the overseas recipient to cooperate with the personal information handler in terms of the inspection by the PRC regulatory authorities, so that the personal information handler is able to effectively assume supervision and inspection responsibilities. Specifically, obligations of the overseas recipient include:

1. **Processing within the agreed scope:** the overseas recipient is required to process the personal information in accordance with the provisions set forth in Appendix I, unless the overseas recipient has obtained prior consent from the personal information subject.

2. **Provide a copy of the Standard Contract:** the overseas recipient should provide a copy of the Standard Contract to personal information subjects upon their request. To the extent necessary to protect trade secrets or other confidential information (such as the contents of protected intellectual property rights etc.), relevant contents may be appropriately redacted. Nonetheless, the overseas recipient must at least provide the personal information subjects with an effective summary to help the personal information subject understand the contents of the Standard Contract.

3. **The principle of minimum necessity:** the personal information to be transferred cross-border is limited to the minimum scope necessary to achieve the purposes of processing.

4. **The principle of minimum retention period:** the overseas recipient must retain the personal information for no longer than necessary for the purpose of processing, unless the personal information subject's separate consent has been obtained.

5. **The principle of secured processing:** the overseas recipient is required to implement effective technical and organizational measures to ensure the security of personal information, ensure that the individuals authorized to process personal information are under the obligation of confidentiality, and establish the minimum necessary access controls.

6. **Respond to data breaches:** in the event of a personal information breach, the overseas recipient is required to adopt timely and appropriate remedial measures to mitigate the adverse impact on the personal information subject, and immediately notify the personal information handler and report to the PRC regulatory authorities in accordance with applicable laws and regulations. Meanwhile, the overseas recipient is required to document and retain all facts related to the data breach and its impact (including all remedial measures adopted).

7. **Strict restrictions on onward transfers of personal information:** the overseas recipient must not provide personal information to any third party located outside the PRC, unless all of the following requirements are met simultaneously:

    - The personal information subject has been informed of the identity and contact information of the third party, the purpose of processing, the method of processing, types of personal information and the manner and procedure for the personal information subject to exercise the rights, and the separate consent from the individual has been obtained, unless applicable laws and regulations stipulate that the individual's separate consent is not required; if any sensitive personal information is involved, the personal information subject has been informed of the necessity to transfer the sensitive personal information and the impact on the individual. When it is difficult to inform the personal information subject or to obtain his or her separate consent, the overseas recipient must promptly inform the personal information handler and request the personal information handler to assist it in informing the personal information subject or obtaining his or her separate consent;

- The overseas recipient has entered into a written agreement with the third party to ensure that the third party's level of personal information protection is not lower than the personal information protection standards stipulated in the applicable PRC laws and regulations.
- The overseas recipient must assume joint and several liability for any damage that may be caused to the personal information subject due to such onward transfer.
- The overseas recipient has provided a copy of the agreement with the third party to the personal information handler.

8. **Reiterates the requirement for the automated decision making**: similar to Article 24 of the PIPL, when using personal information for automated decision making, the overseas recipient must ensure the transparency of decision making and the fairness and impartiality of the results, and must not apply unreasonable differential treatment to individuals in terms of transaction conditions and price. When sending push information and commercial marketing to individuals through automated decision making, the overseas recipient is required to provide options to avoid targeting their personal characteristics or provide a convenient means to refuse.

9. **Cooperate with the personal information handler:** the overseas recipient must make available to the personal information handler all information necessary to demonstrate its compliance with the obligations under, and allow the personal information handler to audit the processing activities under the Standard Contract.

10. **Maintain records of personal information processing activities:** the overseas recipient is required to maintain objective records of the personal information processing activities for at least three years. Meanwhile, the Standard Contract requires that the overseas recipient provide the relevant records and documents to the regulatory authorities directly or through the personal information handler, as required by applicable laws and regulations.

11. **Cooperate with the supervision of the regulatory authorities:** the overseas recipient agrees to submit itself to the jurisdiction of and cooperate with the regulatory authorities during the performance of the Standard Contract, including but not limited to responding to inquiries, cooperating in inspections, complying with the measures adopted or decisions made by the regulatory authorities, and providing written proof that necessary actions have been taken.

In addition to the above obligations, if the overseas recipient is entrusted by the personal information handler to process domestic personal information outside the PRC, it is also required to comply with the following special requirements:

- After the completion of the entrustment, the overseas recipient is required to provide an audit report to the personal information handler upon deletion or anonymization of the personal information.
- In the event of a personal information breach, the personal information handler assumes the obligation to notify the personal information subject.
- When the overseas recipient entrusts a third party to process personal information, the overseas recipient must obtain the consent of the personal information handler in advance. The overseas

recipient is required to ensure that the third party entrusted to process the personal information only processes the personal information within the purposes and methods of processing as agreed in the Standard Contract, and to supervise the personal information processing activities of the third party.

IV. Rights and remedies of personal information subjects

1. The scope of rights

Article 5 of the Standard Contract clarifies that personal information subjects are entitled to most rights stipulated in Chapter 4 of the PIPL, including: the right to know, the right to make decisions, the right to restrict or refuse the processing of their personal information by others, the right of access, the right to copy, the right to correct and supplement, the right to delete, and the right to request an explanation of personal information processing rules. However, the right to "transfer personal information to designated personal information handlers" has not been clearly listed, the conditions of which still need to be further clarified by the CAC.

2. Request rights to which entity

In terms of procedures, the Standard Contract allows the personal information subjects to (i) request the personal information handler to adopt appropriate measures to facilitate his or her exercise of rights, which means the right would be exercised through the domestic personal information handler (and the overseas recipient is obliged to assist), or (ii) directly submit a request to the overseas recipient.

3. Overseas recipient has the right to refuse the unreasonable exercise of rights, but must notify of other remedies

Article 5.4 of the Standard Contract stipulates that if the personal information subject makes excessive or unreasonable requests, especially repeated requests, the overseas recipient may charge a reasonable fee after considering the implementation and operation costs in case the request is approved or refuse to act accordingly. However, if the overseas recipient intends to refuse the personal information subject's request, it must inform the personal information subject of the reasons for the refusal, and the ways for the personal information subject to lodge a complaint with the regulatory authorities and to seek judicial relief. This is also an unprecedented provision made by the CAC to restrict the rights of personal information subjects in its issued documents, which may help personal information handlers to deal with unreasonable requests from personal information subjects.

4. Remedies for personal information subjects and the third party beneficiary clause

The Standard Contract specifies that overseas recipients must designate a contact person to accept and handle complaints from domestic personal information subjects, and to timely notify the personal information handler of disputes with personal information subjects. The personal information subject is also entitled to seek relief from the PRC court or the regulatory authorities, and overseas recipients are required to consent to their jurisdiction.

Similar to the SCC, the Standard Contract also provides that personal information subjects are third-party beneficiaries under the Standard Contract. Personal information subjects are entitled to directly

enforce the terms related to the rights of the personal information subject under the Standard Contract against either the personal information handler or the overseas recipient. Such terms may include some obligations of the personal information handler and the overseas recipient (such as notification and consent, the principle of minimum necessity, data security protection, etc.), assessing the impact of local personal information protection policies and regulations on the compliance with the terms of the Standard Contract, termination clauses, etc. Where the personal information handler or overseas recipient fails to perform contractual obligations, the personal information subject is entitled to file a lawsuit before the people's court with jurisdiction in the PRC and hold them liable for breach of the Standard Contract.

V. Ensure that the law of the country or region where the overseas recipient is located does not affect the performance of the Standard Contract

In 2021, in response to the judgment of the European Union Court of Justice in the Schrems II case, the EU supervisory authority further clarified the application scenario of SCC, requiring data controllers who transfer personal data outside the EU via signing SCC to assess the legislation and practices of third countries in advance. This assessment focuses on legislation and practices of public agency's access to personal data and identifies supplementary measures that need to be adopted. Article 4 of the Standard Contract also draws on this approach, requiring both parties to make reasonable efforts to understand the personal information protection policies and regulations of the country or region where the overseas recipient is located (including any requirements for providing personal information or provisions authorizing public authorities to access personal information), to ensure that laws of the country or region where the overseas recipient is located will not affect overseas recipient's performance of its obligations under the Standard Contract.

Article 4.2 of the Standard Contract specifies the factors to be considered in conducting the assessment, including:

1. the specific circumstances of the export, including the type, quantity, scope and sensitivity of the personal information involved in the transfer, the scale and frequency of the transfer, the duration of transfer and retention of personal information by the overseas recipient, the purpose of personal information processing, the overseas recipient's previous experience with similar exports and processing of personal information, whether the overseas recipient has any data security-related incidents and whether it has dealt with them in a timely and effective manner, whether the overseas recipient has received requests for personal information from public authorities in the country or region where it is located and the overseas recipient's response.

2. the personal information protection policies and regulations of the country or region where the overseas recipient is located, including the following factors: a) the status of existing laws and regulations and generally applicable standards for the personal information protection in such country or region; b) the regional or global organizations on personal information protection of which such country or region is a member, and the binding international commitments it has made; c) the mechanism for the implementation of personal information protection in such country or region, such as whether there is any personal information protection supervision and enforcement body and

relevant judicial body, etc.

3. the security management system and technical means and safeguarding capabilities of the overseas recipient.

In addition, the Standard Contract also stipulates other ancillary obligations in cooperation with the assessment, including that the overseas recipient is required to do its best to provide the personal information handler with necessary relevant information, both parties must record the assessment process and results, and when the personal information protection policies and regulations of the country or region where the overseas recipient is located make it impossible to perform the Standard Contract, the overseas recipient is required to notify the personal information handler immediately upon knowing of such changes.

VI. Termination of the Standard Contract

According to Article 7 of the Standard Contract, the personal information handler is entitled to terminate the Standard Contract when (1) the overseas recipient commits a material or persistent breach of its obligations under the Standard Contract, or (2) when the overseas recipient is subject to bankruptcy, dissolution or liquidation. Apart from the above, either the personal information handler or the overseas recipient may terminate the Standard Contract when: (1) the personal information handler has suspended the transfer of personal information to the overseas recipient for more than one month because the overseas recipient has violated its obligations under the Standard Contract; (2) the overseas recipient's compliance with the Standard Contract may violate the laws of the country or region where it is located; (3) the overseas recipient or the personal information handler has committed a breach of the Standard Contract as identified in a final and non-appealable decision of the competent court or regulatory authorities of the overseas recipient; (4) a decision is made by the regulatory authorities in accordance with applicable laws and regulations regarding the export of personal information, which makes it impossible to execute the Standard Contract.

Notably, according to Article 7.4 and Article 7.5, the termination of the Standard Contract does not release the parties from their obligations to protect personal information in processing activities. Upon the termination of the contract, the overseas recipient will promptly return, destroy, or anonymize the personal information it has received and provide an audit report on the destruction or anonymization.

VII. Liability

In addition to the common liability for breach of contract, Article 8 of the Standard Contract stipulates the division of liability when either party breaches the Standard Contract which causes damages to the personal information subjects:

1. The personal information handler and the overseas recipient assume **joint and several liability** to personal information subjects for any material or non-material damages caused to them due to a breach of the Standard Contract.

2. If one party is held jointly and severally liable to the personal information subjects for a breach by the other party and the party assumes liability in excess of its share, the party will be entitled to seek

recovery from the other party.

Despite the above-mentioned mechanisms for the personal information handler and the overseas recipient to divide any liability arising from breach of the Standard Contract and seek recovery from the other party, it may be difficult for personal information subjects to directly seek compensation from an overseas recipient in practice. Therefore, Article 8.6 of the Standard Contract stipulates that the personal information handler is responsible to the personal information subjects for any material and non-material losses caused by the overseas recipient due to a breach of the Standard Contract, and the personal information subjects have the right to seek recovery from the personal information handler. Therefore, where an overseas recipient commits a breach of the Standard Contract, the personal information handler may first bear all the burden of compensation and then seek contribution from the overseas recipient.

VIII. Dispute resolution and governing law

The Standard Contract clearly stipulates that it is governed by relevant laws and regulations of the PRC. As for dispute resolution, the Standard Contract allows both parties to submit the dispute for arbitration or to a people's court with jurisdiction in the PRC. For the selection of arbitration institutions, the Standard Contract allows both parties to submit disputes to the China International Economic and Trade Arbitration Commission, China Maritime Arbitration Commission, Beijing Arbitration Commission (Beijing International Arbitration Center) and arbitration institutions of other members of the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards. That said, the Standard Contract allows both parties to choose an arbitration institution located in other parties to the New York Convention to settle a dispute related to the Standard Contract, which may allow for overseas recipients to seek a neutral seat of arbitration.

"Ancillary measures" when using the Standard Contracts

The Draft Provisions specify that personal information handlers need to comply with some ancillary compliance obligations and procedural requirements when providing personal information cross-border by signing the Standard Contract. In addition, in order to fulfill the obligations under the Standard Contract, personal information handlers also need to carry out a series of preparations. This section briefly summarizes the "ancillary measures" that personal information handlers need to adopt when signing the Standard Contract as follows:

I. Before signing the Standard Contract

1. **Review existing personal information processing practices and determine whether personal information can be provided cross-border by signing the Standard Contract.** According to Article 4 of the Draft Provisions, personal information handlers will determine whether they may provide personal information cross-border by signing the Standard Contract from the perspective of "whether the personal information handler is a CIIO", "the amount of personal information processed" and "the cumulative amount of personal information and sensitive personal information that have been provided cross-border since January 1 of the previous year".

2. **Review the facts about the export of personal information.** The personal information handler should clarify the types of personal information subjects involved in the export of personal information, the purpose, quantity, method of the export of personal information, types of personal information, types of sensitive personal information, the recipient of the personal information provided by the overseas recipient, the retention period and the retention location after the export, whether the overseas recipient will entrust third parties to process personal information or transfer personal information to other third parties, and other related matters, in order to perform the obligation of conducting the personal information protection impact assessment required in Article 5 of the Draft Provisions and fill in the Appendix I when signing the Standard Contract.

3. **Check whether sufficient compliance measures have been adopted.** Considering that the Standard Contract requires personal information handlers to make statements, warranties and covenants about their obligations, once personal information handlers violate the contract in the subsequent export of personal information, they may be investigated and punished by regulatory authorities and even be required by overseas recipients to bear the corresponding liability for breach of the contract. Therefore, before signing the Standard Contract, it is advisable for personal information handlers to prepare for the personal information protection impact assessment, in accordance with the obligations of personal information handlers required in the PIPL and Article 2 of the Draft Provisions, including, among others, informing the individuals and obtaining their separate consent.

4. **Assess the personal information protection capabilities of overseas recipients in advance.** In view that the Standard Contract regards personal information handlers as the primary object of the competent authorities to supervise the export of personal information and the personal information protection capabilities of overseas recipients may affect the results of the personal information protection impact assessment, it is recommended that personal information handlers assess the personal information protection capabilities of overseas recipients in accordance with the obligations of the overseas recipients required in Article 3 of the Draft Provisions one by one before providing personal information cross-border to mitigate the relevant compliance risks.

5. **Investigate and evaluate the impact of personal information protection policies and regulations in overseas countries or regions on compliance with the terms of the Standard Contract.** According to Article 4 of the Standard Contract, both parties must make reasonable efforts to understand whether the personal information protection policies and regulations of the country or regions where the overseas recipient is located will prevent the overseas recipient from performing its obligations under the Standard Contract. With reference to the relevant practices of GDPR, personal information handlers may draft a questionnaire about the personal information protection policies and regulations in recipients' countries or regions, learn about the local personal information protection policies and regulations through overseas recipients or local counsels, and make assessments based on the recipient's personal information protection capabilities.

6. **Conduct personal information protection impact assessments and retain records.** On the basis of the above steps (2)-(5), personal information handlers should carry out personal information protection impact assessments and retain such records for at least three years in accordance with

Article 55 of the PIPL and the Draft Provisions[4]. Meanwhile, in light of the requirements of the PIPL, the Draft Assessment Measures and the *Information Security Technology- Guidelines for Data Cross-Border Transfer Security Assessment (Draft for Comments)*, personal information handlers may conduct impact assessments in two steps, including assessing the purpose of the export and assessing the security risk. When assessing the purpose of the export, personal information handlers may determine whether the purpose of the export is compliant with the requirements of legality, legitimacy and necessity at the same time. When assessing the security risk, personal information handlers may consider the factors including the types, quantity, scope, sensitivity of personal information to be provided, corresponding technical security measures to be adopted, data security protection capabilities of the domestic personal information handler and the overseas recipient.

II. After signing the Standard Contract

1. **File a record with the local provincial CAC within 10 working days from the effective date of the Standard Contract.** According to Article 7 of the Draft Provisions, personal information handlers are required to file with a provincial-level CAC within 10 working days from the effective date of the Standard Contract and submit the following materials: (1) the Standard Contract; and (2) the personal information protection impact assessment report. It should be noted that Article 7.2 of the Draft Provisions also specifies that after the Standard Contract comes into effect, personal information handlers may export personal information. That said, completing the filing procedures does not constitute a precondition for exporting personal information. However, personal information handlers are responsible for the authenticity of the filed materials.

2. **Provide a copy of the signed Standard Contract to the personal information subjects at their request.** According to Article 2 of the Standard Contract, when personal information subjects request the personal information handler to provide a copy of the Standard Contract signed between the personal information handler and the overseas recipient, the personal information handler must provide a copy of the Standard Contract or provide a redacted version, for purposes such as protecting trade secrets. Personal information handlers are required to undertake that they will provide the personal information subjects with an effective summary to help them understand the contents of the Standard Contract.

3. **Update privacy policies or other notification documents.** In order to fulfill the obligations of providing a copy of the Standard Contract to personal information subjects and providing convenient

[4] Personal information protection impact assessments focus on the following aspects: (1) the legality, legitimacy, and necessity of the purpose, scope, and method of the personal information processing by the personal information handler and the overseas recipient;
(2) the quantity, scope, type, and sensitivity of personal information to be transferred cross-border, and the risk that the export of personal information may bring to personal information rights and interests;
(3) the responsibilities and obligations that the overseas recipient undertakes to assume, and whether its management and technical measures and capabilities to fulfill such responsibilities and obligations are sufficient to ensure the security of personal information to be transferred cross-border;
(4) risks of data leakage, damage, tampering, abuse, etc. after the export of personal information, and whether the channels for individuals to maintain personal information rights and interests are unblocked, etc.;
(5) the impact of personal information protection policies and regulations in the country or region where the overseas recipient is located on the performance of the Standard Contract; and
(6) other matters that may affect the security of personal information to be transferred cross-border.

channels for personal information subjects to exercise their rights, personal information handlers need to update their privacy policy or other notification documents, and clearly inform the individual of the method to obtain the copy of the Standard Contract and to exercise their rights to personal information handlers or overseas recipients.

4. **Continuously monitor the export of personal information, and re-sign the Standard Contract with the overseas recipient in the event of specified circumstances.** Article 8 of the Draft Provisions stipulates three circumstances where personal information handlers are required to re-sign the Standard Contract and file a record, including: (1) there is any change to the purpose, scope, type, sensitivity, quantity, method, retention period, and retention location of the personal information transferred cross-border, or any change to the purpose and method of the overseas recipient for handling personal information, or an extension of the overseas retention period of the personal information; (2) there is any change to personal information protection policies and regulations in the country or region where the overseas recipient is located, which may affect personal information rights and interests; (3) there are other circumstances that may affect personal information rights and interests.

5. **Retain personal information export records and relevant written documents.** Considering that personal information handlers have to bear the burden of proof for proving that they have fulfilled their obligations under the Standard Contract, personal information handlers should pay attention to keeping and filing documents related to the export of personal information, such as assessment records of local personal information protection policies and regulations, and personal information protection impact assessment records.

6. **Cooperate with inspections conducted by regulatory authorities.** According to Article 11 of the Draft Provisions, where a CAC at or above the provincial level finds that any activity related to the export of personal information by way of signing the Standard Contract no longer meets the security management requirements for the export of personal information during the actual processing, it will notify the personal information handler in writing to terminate the export of personal information. The personal information handler must immediately terminate the export of personal information upon receipt of the notice. In addition, Article 12 of the Draft Provisions also provides that in circumstances where (i) personal information handlers fail to comply with the record-filing procedure or submit false materials for record-filing; (ii) personal information handlers fail to fulfill any responsibilities or obligations stipulated in the Standard Contract and infringes personal information subjects' rights and interests and causes any harm; or (iii) other circumstances that may affect personal information subjects' rights and interests, the CAC at or above the provincial level will order corrections within a time limit in accordance with the PIPL; if the personal information handler refuses to make rectifications or the personal information rights and interests are harmed, it will be ordered to terminate the export of personal information and be subject to penalties in accordance with the law; if a crime is constituted, criminal liability will be investigated in accordance with the law.

Summary and outlook

In short, although the Standard Contract provides a mechanism for personal information handlers to

transfer personal information cross-border without carrying out security assessments by CAC, its application is neither simple nor easy. Personal information handlers need to be fully prepared to establish cross-border data compliance governance mechanisms including notification and consent, responses to users' rights, data security protection, supervision and management of overseas recipients, research and tracking of the legal documents of overseas recipients' countries and regions, etc., in order to successfully export personal information.

In addition, based on the fundamental legal framework for the export of personal information established by the PIPL, the CAC issued the Draft Assessment Measures last year, and the National Information Security Standardization Technical Committee also released this year the *Technical Specifications for the Certification of Personal Information Cross-border Processing*. With the gradual implementation of relevant regulations, the compliance scheme for China's cross-border personal information transfer will gradually become clear and feasible. It is advisable for both Chinese companies with overseas business and foreign companies operating in China to keep a close eye on the relevant legislative developments and design reasonable and feasible compliance plans for the export of personal information as soon as possible.

Important Announcement

This Newsletter has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Beijing	**Wenyu JIN**	**Attorney-at-law**
	Tel:	+86 10 8525 5557
	Email:	wenyu.jin@hankunlaw.com
Shanghai	**Yinshi CAO**	**Attorney-at-law**
	Tel:	+86 21 6080 0980
	Email:	yinshi.cao@hankunlaw.com
Shenzhen	**Jason WANG**	**Attorney-at-law**
	Tel:	+86 755 3680 6518
	Email:	jason.wang@hankunlaw.com
Haikou	**Jun ZHU**	**Attorney-at-law**
	Tel:	+86 898 3665 5000
	Email:	jun.zhu@hankunlaw.com
Wuhan	**Jiao MA**	**Attorney-at-law**
	Tel:	+86 27 5937 6200
	Email:	jiao.ma@hankunlaw.com
Hong Kong	**Dafei CHEN**	**Attorney-at-law**
	Tel:	+852 2820 5616
	Email:	dafei.chen@hankunlaw.com