JUNHE BULLETIN

2021 年 11 月 23 日

Hot Topics Regarding Personal Information Protection Laws

Some key poins of the regulations on network data security management (draft for comments) – data cross-border transfer

On November 14, 2021, the *Regulations on Network Data Security Management (Draft for Comments)* ("**Draft Data Security Regulations**") was released by the Cyberspace Administration of China ("**CAC**") and made available to the public for comment until December 13, 2021

The Draft Data Security Regulations was drafted based on the *Cybersecurity Law*, the *Data Security Law* and the *Personal Information Protection Law* ("**PIPL**") as the superordinate laws. It consists of 75 articles in nine chapters, addressing many key points in detail such as the safe cross-border transfer of data, the protection of personal information rights, the cybersecurity review standards for IPOs in foreign countries or Hong Kong, and the obligations of internet platform operators. We will discuss the Draft Data Security Regulations in a series of updates and topics. In this article, we focus on cross-border transfers of data.

1. Prerequisites for Exports of Data and Exemptions

The first paragraph of Article 35 of the Draft Data Security Regulations generally reiterates the prerequisites for the cross-border transfer of personal information stipulated in Article 38 of the PIPL and extends their application to all network data as follows: (1) the data processor has passed the data export security assessment organized by the national cyberspace administration; (2) both the data processor and the data recipient have been certified for the protection of personal information by a professional institution accredited by the national cyberspace administration; and (3) the data processor has entered into a contract with the data recipient outside the territory of China in accordance with the standard contract regulations established by the national cyberspace administration to set forth the rights and obligations of both parties. It is provided for in

Article 35(2) of the Draft Data Security Regulations that the above prerequisites can be exempted if: the data processor provides the personal information of an individual to a recipient outside the territory of China (1) as is necessary for the conclusion or performance of a contract to which such individual is a party, or (2) as is necessary for the protection of the life, health and property of such individual.

According to the above regulations, data processors are required to meet one of the three prerequisites for the data cross-border transfer, regardless of whether the data they transfer abroad contains any personal information, core data or important data. This imposes higher compliance requirements on data export practices by enterprises. As for the required standard contract, the national cyberspace administration has not yet issued any standard contract applicable to the export of personal information. Also, the aspects an enterprise should focus on in their security assessments and contracts with respect to the export of data other than personal information, core data and important data are subject to further clarification in the relevant regulations.

The exemption of data exports that are "necessary for the conclusion or performance of a contract" and are "necessary for the protection of the life, health and property of such individual" can facilitate a data export, but their exact scope needs further clarification. For example, if a domestic user uses an app/mini program developed by a foreign company to acquire services, or if an international company provides global services to consumers, whether the said exemption provisions can apply is subject to further clarification. In addition, the Draft Data Security Regulations does not explicitly set forth any clear provisions on data localization.

2. Separate Consent for the Export of Personal Information and the Timing for Obtaining Consent

Article 36 (1) of the Draft Data Security Regulations reiterates the separate consent required for the export of personal information under Article 39 of the PIPL as follows: where a data processor provides the personal information of an individual to a recipient outside the territory of People's Republic of China, the data processor shall inform such individual of the name and contact details of the overseas data recipient, the purpose of the processing, the manner of the processing, the type of personal information, and the manner in which the individual can exercise their rights in his/her personal information against the overseas data recipient, and obtain separate consent from such individual.

As for the relationship between the separate consent required for the export of personal information and the exemption of data exports that are "necessary for the conclusion or performance of a contract to which the individual is a party" under Article 13(1)(ii) of the PIPL, there have been different views on whether separate consent is required or not for the export of personal information if the export is "necessary for the conclusion or performance of a contract to which the individual is a party". The government authority has not provided a clear explanation yet. The Draft Data Security Regulations also does not clearly address this issue.

Article 36(2) of the Draft Data Security Regulations separately provides that "If separate

consent for the export of personal information has been obtained from the individual at the time of collection of such personal information, and the export of personal information complies with the matters for which consent is obtained, no separate consent is required to be obtained again from the individual." According to this provision, if a company has already obtained separate consent from an individual for the export of personal information at the time of collection thereof, it is not necessary to obtain separate consent from the individual again before a subsequent export.

3. Data Export Security Assessment

Article 37 of the Draft Data Security Regulations sets out the following circumstances that are subject to the data export security assessment organized by the national cyberspace administration: (1) the data transferred abroad contains important data; and (2) critical information infrastructure operators, or data processors who process the personal information of more than one million individuals, provide personal information to a recipient outside the territory of China.

The "one million" threshold mentioned in the second circumstance above echoes Article 13 of the Draft Data Security Regulations and Article 6 of the *Cybersecurity Review Measures (Draft Revised for Public Comments)* released by the CAC on 10 July 2021[1], which requires a data processor to apply for a cybersecurity review if it falls into the circumstance of "the overseas listing of a data processor that processes the personal information of more than one million individuals". However, it is noteworthy that the Draft Data Security Regulations does not reiterate the requirement that "any provision of the personal information of more than 100,000 individuals or the sensitive personal information of more than 10,000 individuals to recipients outside of China in aggregate" shall be subject to a security assessment as stipulated in the *Data Export Security Assessment Measures (Draft for Comments)* issued by the CAC on 29 October 2021[2]. In addition, the Draft Data Security Regulations does not specify the validity period of the data export security assessment.

Data processors who violate the compliance obligations listed above may face penalties in accordance with Article 64 of the Draft Data Security Regulations, including government orders to suspend data exports and impose monetary fines of up to RMB 10 million for companies and RMB 1 million for responsible personnel. In particular, (1) the relevant authority will order rectification, issue warnings, suspend the data export, and may at its discretion impose a fine of at least RMB 100,000 and up to RMB 1 million against the data processor and at least RMB 10,000 and up to RMB 100,000 against the officers and other personnel of the data processor who are directly liable for the violation; (2) in case of a grave violation, the relevant authority will impose a fine of at least RMB 1 million and up to RMB 10 million, and may at its discretion order the data processor to suspend any related business

[1] The *Cybersecurity Review Measures (Draft Revised for Public Comments)* released by the CAC can be found at http://www.cac.gov.cn/2021-07/10/c_1627503724456684.htm.

[2] The notice of the CAC on the release of the *Data Export Security Assessment Measures (Draft for Comments)* for public comments can be found at http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm.

activity or to suspend business until rectification, revoke the related business permit or business license of the data processor, and impose a fine of at least RMB 100,000 and up to RMB 1 million against the officers and other personnel of the data processor who are directly liable for the violation.

4. Annual Reporting Obligations to CAC Regarding Data Exports

Under Article 40, the Draft Data Security Regulations impose reporting obligations on data processors who process any personal data or important data for preparing and submitting a data export security report regarding data exports in the previous year to the municipal cyberspace administration of a city having districts by January 31 each year, and such a report should include: (1) the name and contact details of each data recipient involved; (2) the type, amount and purpose of data transferred abroad; (3) the place and period of storage and scope and means of use of the data abroad; (4) the complaints lodged by users regarding the transfer of their data abroad and related resolutions; (5) the data security incidents that occurred and their handling; and (6) the retransfer of the data transferred abroad.

The Draft Data Security Regulations are short on waivers of such reporting obligations. This means that in practice, it is the obligation of any company that transfers personal information outside of China. In accordance with Article 64 of the Draft Data Security Regulations, non-compliant data processors may face penalties including government orders to suspend data exports and monetary fines of up to RMB 10 million for companies and RMB 1 million for responsible personnel. Please refer to Section 3 "Data Export Security Assessment" for more details regarding the statutory provisions for the penalties and sanctions imposed.

The *Regulations on Automobile Data Security Management (for Trial Implementation)* also introduce, under Article 14, the reporting requirements for automobile data processors transferring important data outside of China. Although having substantially consistent provisions with Article 40 of the Draft Data Security Regulations, the Automobile Data Security Regulations introduce additional reporting requirements on automobile data processors to provide a statement of the necessity for transferring automobile data outside of China and report such information as required by CAC in conjunction with the relevant administrative authorities of industry and information technology, public security and transport, etc. In this regard, uncertainties still exist in relation to the harmonization of the requirements outlined in Article 40 of the Draft Data Security Regulations with the provisions of the *Regulations on Automobile Data Security Management (for Trial Implementation)* previously issued regarding the data export security assessment.

5. Other Obligations Related to Data Exports

Article 39 of the Draft Data Security Regulations clarify the obligations of data processors when transferring data outside of China. In addition to the specific rules regarding cross-border data transfers indicated in Chapter 3 of the PIPL, the following newly adopted requirements set forth under Article 39 are noteworthy:

1) Where the data export causes any

damage to the legitimate rights and interests of individuals or organizations or to the public interest, the data processor shall be held liable in accordance with the law. This means that the data processor would accept joint and several liability for the damages caused by the data recipients.

2) Records of the logs and approvals related to data exports shall be kept for at least three years. The three-year time requirement is consistent with the retention period of personal information assessment reports provided for under the PIPL.

3) If the national cyberspace administration determines that the data shall not be transferred abroad, the data processor shall stop the cross-boarder transfer of the data and take effective measures to remedy the security of the data that has been transferred abroad.

4) Where it is necessary to re-transfer personal information after it has been transferred abroad, the data processor shall agree in advance with the individual on the conditions for the re-transfer and specify the security protection obligations required to be performed by the data recipient. Article 9 of the *Measures on Security Assessment of Data Export (Draft for Comments)* provides that the contract between the data processor and the overseas recipient shall contain a provision that restricts an overseas recipient from retransferring the data transferred to it to any other organization or individual. This "restrictive provision" echoes the provision of Article 39 under the Draft Data Security Regulations regarding the agreement "with the individual on the conditions for re-transfer" and can be used as a reference by data processors when designing such a "restrictive provision".

6. Setup of "Export Data Security Gateways" and Regulations on the Use of Illegal VPNs

Article 41 of the Draft Data Security Regulations explicitly provides that the government will set up a national "cross-border data security gateway" to block the flow of foreign-originated illegal information. Any person who provides programs, tools, routes or services, including internet access, server hosting, technical support, marketing and promotion, payment and settlement or application downloads, for penetrating and bypassing cross-border data security gateways will face penalties in accordance with Article 66 of the Draft Data Security Regulations, including monetary fines of up to ten times the value of the illegal gains or RMB 500,000 in the absence of illegal gains.

Despite the legal framework established by the Regulation on Telecommunications and other existing laws and regulations for international network services from the aspects of license grants and usage specifications, the Draft Data Security Regulations expressly prohibits the illegal cross-border programs, tools, routes and other services for the first time and imposes more

severe penalties for breaches.

In addition to the specific requirements for cross-border data transfers addressed above, the Draft Data Security Regulations further refine and build upon the regulatory provisions for the protection of the rights of individuals to personal information, the criteria for cybersecurity review for listing abroad and listing in Hong Kong, as well as the obligations of Internet platform operators. We will discuss these topics in future articles.

Marissa Dong	Partner	Tel：86 10 8519 1718	Email：dongx@junhe.com
Jinghe Guo	Associate	Tel：86 10 8553 7947	Email：guojh@junhe.com
Shuoying Li	Associate	Tel：86 21 2208 6242	Email lishuoyin@junhe.com