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

Han Kun Newsletter

Issue 170 (6th edition of 2021)

Legal Updates

1. A New Chapter in Data Security Governance – Commentary on the Data Security Law
2. Brief Comments on Draft Automobile Data Security Provisions

1. A New Chapter in Data Security Governance – Commentary on the Data Security Law

Authors: Kevin DUAN | Kemeng CAI | Minzhe HU[1]

On June 10, 2021, the *Data Security Law of the People's Republic of China* (the "**Data Security Law**") was adopted at the 29th meeting of the Standing Committee of the 13th National People's Congress. The law will officially enter into force on September 1, 2021. The Data Security Law is a fundamental law in the area of data security and is also a key component of the entire national security legal system. In this article, we provide a preliminary analysis of the changes and key issues in the final draft of the Data Security Law, and then further analyze the relationship between the Data Security Law and other related regulations as well as challenges for corporate compliance.

What are the important changes compared to the second reading draft?

The final draft of Data Security Law is generally consistent with the April 29 second reading draft that preceded it. The primary changes are as follows:

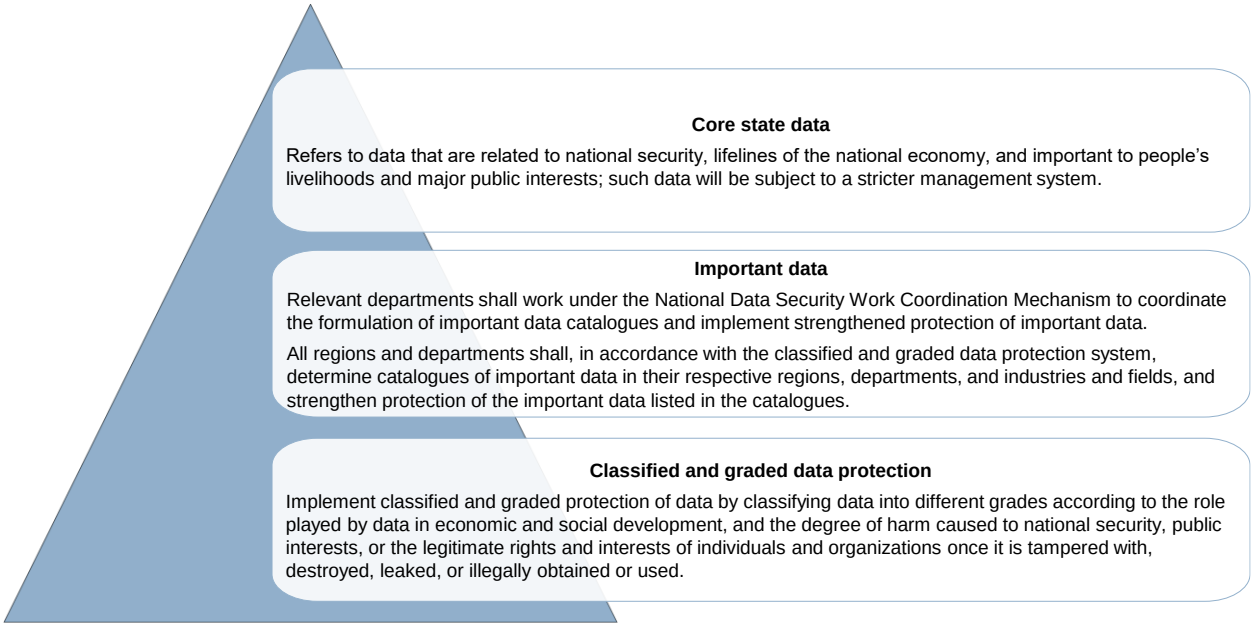
- **Strengthens the top-level design of data security management.** According to Article 5 of the final draft, the National Security Commission of the CPC will coordinate major issues and work related to national data security. The article also establishes a coordination mechanism for national data security work and strengthens the top-level design of data security management.
- **Core state data appears for the first time, strengthening classified and graded data protection.** The final draft at Article 21 introduces the concept of "core state data" based on the establishment of classified and graded data protection systems and the development of an important data catalogue. In this regard, the Article 21 provides that core state data is "data related to national security, lifelines of the national economy, important matters related to people's livelihood and major public interests and such data will be subject to a stricter management system."
- **Strengthens the management for provision of data to overseas institutions, raises maximum penalties.** The second reading draft for the first time stipulated penalties for companies that unlawfully provide domestic data to overseas law enforcement agencies and judicial authorities. The final draft at Article 48 significantly raises the maximum penalties for enterprise violations – if an enterprise provides domestic data to overseas law enforcement agencies and judicial authorities and causes serious consequences, it may be subject to a fine of up to RMB 5 million, and may be ordered to suspend its relevant business, close business for rectification, and may have its relevant business permits or business licenses revoked. Persons in charge and others directly responsible may be subject to fines of up to RMB 500,000.

[1] Intern Zihuan XU has also contributed to the writing of this article.

- **Advances requirements to adapt to the needs of the elderly, ensuring the digital rights and interests of the elderly.** Since last year, the Ministry of Industry and Information Technology has successively issued plans requiring internet websites and mobile apps to better accommodate the needs of the elderly, including the *Special Action Plan for Aging People Adaptation and Barrier-free Transformation of Internet Applications*, and the *Circular on Further Implementing the Special Action Plan for Aging People Adaptation and Barrier-free Transformation of Internet Applications*. The final draft at Article 15 adapts to the aging demographic trend in Chinese society, stipulating for the first time under law to "take into account the needs of the elderly" and requiring providers of intelligent public services take into full consideration the needs of the elderly and the disabled and to ensure accessibility for these groups.

What are the grades of data protection?

The Data Security Law sets forth the concept of "core state data," based on the establishment of classified and graded data protection systems and the development of an important data catalogue, and stipulates a complete graded data protection system by grading data in terms of importance. Based upon the Data Security Law, data is to be graded and protected according to the following:



What important supporting systems does the Data Security Law establish?

The Data Security Law establishes basic systems for data protection, laying a foundation for data security management and protection as well as administration of data circulation and application in China. These basic systems mainly include:

- **Data transaction management system**: China will establish a data transaction management system, in order to standardize data transactions and facilitate development of the data transactions market (Article 19). Agencies that provide data trading intermediary services must request data providers to explain their data sources, verify the identities of both transaction parties, and maintain verification and transaction records (Article 33).

- **Important data protection system**: The Data Security Law puts forward special requirements for the processing of important data. These requirements include: processors of important data must specify the person(s) responsible for important data security and the relevant responsible department, and should undertake responsibilities for data security protection (Article 27); processors of important data must regularly conduct risk assessments of their data processing activities in accordance with the relevant provisions and submit risk assessment reports to the relevant competent authorities. Risk assessment reports are to specify the types and quantities of important data processed, the description of the data processing activities, and the data security risks possibly arising from the data processing activities and the countermeasures thereto (Article 30).

- **Data security risk management and control system**: China will establish centralized, unified, efficient, and authoritative data security risk assessment, reporting, information sharing, monitoring, and early warning mechanisms. China will also establish a national data security work coordination mechanism, under which the relevant departments will cooperate to strengthen the work of acquiring, analyzing, researching, judging, and early warning of data security risk information (Article 22).

- **Data security emergency response mechanism**: China will establish a data security emergency response mechanism. Under this mechanism, in the event of a data security incident, the relevant competent authorities will activate an emergency response plan in accordance with law and take appropriate emergency response measures to prevent the spread of damage, eliminate potential security risks, and promptly give warnings to the public (Article 23).

- **Data security review system**: China will establish a data security review system, under which data processing activities that affect or may affect national security will be subject to national security review. Decision made by the relevant departments on data security reviews in accordance with the law will be final. This means that the data security review system will exclude remedies such as administrative review and administrative litigation (Article 24).

What important systems govern cross-border data exchanges?

- **CII operators obligated to localize data**: According to the Data Security Law, the cross-border transfer of important data collected and generated in the operation of critical information infrastructure ("**CII**") within China is governed by the Cybersecurity Law (Article 31). According to Article 37 of the Cybersecurity Law, personal information and important data collected and generated in the operation of CII in China must be stored in China. If it is necessary to provide such data and information to overseas parties due to business needs, a security assessment must be conducted in accordance with the measures jointly formulated by the national cyberspace administration and relevant departments under the State Council, unless otherwise provided by laws and administrative regulations.

- **Cross-border data transfers by other data processors to be subject to administrative rules issued by the cyberspace administration and other authorities**: The cyberspace administration

and relevant departments under the State Council will formulate administrative measures for the security review of cross-border transfers of important data collected and generated during the operation of facilities within China (Article 31). After the adoption of the Data Security Law, relevant supporting regulations will be successively formulated and improved so as to provide clear guidance to data operators.

- **Requests for domestic data by overseas law enforcement or judicial authorities**: Chinese competent authorities will process requests for domestic data from overseas law enforcement or judicial authorities in accordance with relevant laws and international treaties or agreements concluded or acceded to by China, or in accordance with the principles of equality and mutual benefit. No organization or individual within China may provide overseas law enforcement or judicial authorities with data stored in China without the approval of the Chinese competent authorities (Article 36).
- **Data export control system**: China will implement export controls over data that is categorized as a controlled item and is relevant to safeguarding national security and interests and to fulfilling international obligations (Article 25).
- **Anti-discrimination system**: Where any country or region takes, on discriminatory basis, prohibitive, restrictive, or other similar measures against China in terms of investment or trade related to data, data development, and technology utilization, etc., China may take reciprocal measures against such country or region according to actual circumstances (Article 26).

Important enterprise data security compliance obligations

Under the Data Security Law, enterprises have the following primary obligations in terms of data compliance and may be subject to the following punishments in the event of violation of relevant obligations.

Article	Obligations	Punishments for violation
Article 27 Data security protection obligations and important data security protection obligations	In order to conduct data processing activities, enterprises shall establish a sound data security management system, organize data security education and training, and take appropriate technical measures and other necessary measures in accordance with laws and regulations, so as to protect data security. When data processing activities are conducted through information networks such as the Internet, the above data security protection obligations shall also be followed, subject to compliance with requirements under the classified data protection system. Processors of important data shall specify the person(s) responsible for data security and the department in charge of data security protection.	**In general:** (1) Enterprises: ■ Corrections; ■ Warnings; ■ Fines of RMB 50,000-500,000. (2) Persons in charge and others directly responsible: ■ Fines of RMB 10,000-100,000. **In cases of refusal to make corrections or the violation results in serious consequences, such as a large data leakage:** (1) Enterprises: ■ Fines of RMB 500,000-2,000,000; and ■ Being ordered to suspend relevant business or to close for rectification; ■ Revocation of relevant business operating
Article 29 Risk monitoring and	Enterprises shall strengthen risk monitoring when conducting data processing activities and shall take remedial measures immediately upon discovery of data security defects, bugs, and other risks. In the	

Article	Obligations	Punishments for violation
emergency response	event of a data security incident, enterprises shall take responsive measures in accordance with regulations, notify users, and report to the relevant competent authorities immediately in accordance with law.	permits or business licenses. (2) Persons in charge and others directly responsible: ■ Fines of RMB 50,000-2,000,000.
Article 30 Risk assessment and reporting of important data	Processors of important data shall, in accordance with regulations, conduct risk assessment of their data processing activities on a regular basis and submit risk assessment reports to the relevant competent authorities. A risk assessment report shall specify the types and quantities of important data processed, descriptions of data processing activities, data security risks possibly arising and the countermeasures therefor.	
Article 21 Core state data protection obligations	Core state data refers to data relating to national security, lifelines of the national economy, and that is important to people's livelihoods and major public interests, and such data shall be subject to a stricter management system.	■ Fines of RMB 2 million-10 million; ■ Being ordered to suspend relevant business or to close for rectification; ■ Revocation of relevant business operating permits or business licenses; ■ If a crime is constituted, criminal liability shall be investigated in accordance with the law.
Article 31 Restrictions on the cross-border provision of important data	If an operator of critical information infrastructure intends to export important data collected and generated in the operation of critical information infrastructure within the territory of China, the Cybersecurity Law of the People's Republic of China shall apply. The export of other important data collected and generated within the territory of China shall subject to management of administrative regulations formulated by the cyberspace administration authority together with relevant departments under the State Council.	**In general:** (1) Enterprises: ■ Corrections; ■ Warnings; ■ Fines ranging from RMB 100,000 to 1 million. (2) Persons in charge and others directly responsible: ■ Fines ranging from RMB 10,000 to 100,000. **In serious cases:** (1) Enterprises: ■ Fines ranging from RMB 1 million to 10 million; ■ Being ordered to suspend relevant business or to close for rectification; ■ Revocation of relevant business operating permits or business licenses. (2) Persons in charge and others directly responsible: ■ Fines ranging from RMB 100,000 to 1 million.
Article 33 Obligations of data transaction intermediary service providers	Agencies that provide data transaction intermediary services shall request data providers to explain data sources, verify the identities of both transaction parties, and maintain verification and transaction records.	(1) Enterprises: ■ Corrections; ■ Confiscation of illegal gains; ■ Imposition of fines ranging from one to ten times the illegal gains; if there are no illegal gains or the illegal gains are less than RMB

Article	Obligations	Punishments for violation
for data source review and maintenance of transaction records		100,000, a fine ranging from RMB 100,000-1 million shall be imposed; ■ Being ordered to suspend relevant business or to close for rectification; ■ Revocation of relevant business operating permit or business license. (2) Persons in charge and others directly responsible: ■ Fines ranging from RMB 10,000 to 100,000.
Article 35 Cooperation in the provision of data	Where public security organs or national security organs need certain data to be provided for purposes of safeguarding national security or investigating crimes in accordance with the law, they shall, in accordance with the relevant provisions of the State, strictly go through approval procedures, and relevant organizations or individuals shall cooperate with the provision of data.	(1) Enterprises: ■ Corrections; ■ Warnings; ■ Fines ranging from RMB 50,000 to 500,000. (2) Persons in charge and others directly responsible: ■ Fines ranging from RMB 10,000 to 100,000.
Article 36 No data may be provided to foreign judicial or law enforcement authorities without approval of the Chinese competent authorities	The Chinese competent authorities shall process requests for the provision of data from foreign judicial or law enforcement authorities in accordance with relevant laws and international treaties or agreements concluded or acceded to by China, or in accordance with the principles of equality and mutual benefit. No organization or individual within the territory of China may provide foreign judicial or law enforcement authorities with data stored within the territory of the China without the approval of the Chinese competent authorities.	**In general:** (1) Enterprises: ■ Warnings; ■ Fines ranging from RMB 100,000 to 1 million. (2) Persons in charge and others directly responsible: ■ Fines ranging from RMB 10,000 to 100,000. **In serious cases:** (1) Punishments for enterprises include: ■ Fines ranging from RMB 1 million to 5 million; ■ Being ordered to suspend relevant business or to close for rectification; ■ Revocation of relevant business permits or business licenses. (2) Persons in charge and others directly responsible: ■ Fines ranging from RMB 50,000 to 500,000.

Conclusion

The Data Security Law systematically echoes the requirements of pursuing a holistic approach to national security and comprehensively establishing a basic legal framework for data security governance. However, the Data Security Law mainly specifies the general principles and direction for data security governance and does not generally address detailed rules and obligations. Therefore, the regulatory authorities will need to further formulate supporting rules and regulations in order to assist with implementation of important systems under the law. It also remains to be further clarified the relationships among these systems, including the data security protection system, important data protection system, data security incident and emergency response system, anti-discrimination system, data export control

system, data security review system, and other relevant systems and measures, particularly those under the Personal Information Protection Law, the Cybersecurity Law, the Anti-foreign Sanctions Law, the Export Control Law, the Foreign Investment Law, and the Measures for Examination of Cybersecurity, among others. We foresee these relevant supporting rules being soon released with the gradual implementation of the relevant systems. We recommend companies to closely watch legal developments in this area and prepare to make the changes necessary to come into compliance.

2. Brief Comments on Draft Automobile Data Security Provisions

Authors: Kevin DUAN | Tina WANG | Kemeng CAI[2]

On May 12, the Cyberspace Administration of China ("**CAC**") issued for public comments the *Several Provisions on Administration of Automobile Data Security (Draft for Comment)* ("**Draft Provisions**"). The Draft Provisions would be the first departmental rules dedicated to addressing data compliance requirements in the automobile industry. Unlike previous draft standards[3] proposed for connected vehicles, the Draft Provisions would apply to vehicles of all types. The key take-aways of the Draft Provisions are as follows:

- Defines the scope of important data in the automobile industry. The processing of important data would be subject to a series data protection principles and requirements such as data minimization, vehicle-end processing, data localization and export security assessment, and government filing and annual reporting.
- Emphasis on ensuring data subjects' control of personal information ("**PI**") collection and deletion.
- Strengthening of obligations to report data processing activities to regulatory authorities.
- Potential changes to industry practices. The Draft Provisions would require significant changes to current vehicle data processing designs and practices due to their requirements with respect to data minimization, vehicle-end processing, data subject control, and data localization.

Below, we analyze the key requirements for PI and important data processing provided in the Draft Provisions and offer our insights accordingly.

Applicable scope

According to Articles 2 and 3, the Draft Provisions apply to the processing of PI and important data by operators in relation to the design, manufacture, sale, operation and maintenance, and management of vehicles within China. Operators under the Draft Provisions include vehicle manufacturers, suppliers of parts and software, distributors, maintenance workshops, online ride-hailing enterprises, insurance companies, and other enterprises and institutions in the areas of vehicle design, manufacture, and services In other words, almost all entities in the automobile industry could fall into the ambit of the Draft Provisions when they process important data and PI, including of vehicle owners, drivers and passengers, and pedestrians.

Yet, it is unclear whether the Draft Provisions would apply to internal data processing activities that are unrelated to automobile management, such as the processing of employee PI. In addition, the Draft Provisions do not yet specify whether and how they would apply to vehicles that are already in the market

[2] Intern Shimeng CAI has also contributed to the writing of this article.

[3] E.g., *Draft Information Security Technology – Connected Vehicle – Security Requirements of Data* published by the National Information Security Standardization Technology Committee on April 28.

or currently in production.

Scope of important data

Article 3 of the Draft Provisions defines the scope of important data in the automobile industry, which would include:

- Crowd and traffic data in important and sensitive areas such as military administrative zones, areas in the vicinity of science, technology, and national defense agencies and other State secret-related agencies, and areas in the vicinity of Party and government agencies above the county level;
- Surveying and mapping data, the precision of which is above maps made public by the State;
- Data on the operation of vehicle charging networks;
- Data on vehicle types and road traffic;
- Outside-vehicle audio and video data including human faces, voices, vehicle license plates, etc.;
- Other types of data that might impact national security and public interests as designated by the State cyberspace administrations and departments of the State Council.

Detailed criteria are yet to be specified as to how to draw the scope of important data in practice, such as how to calculate crowd and traffic data, how to identify important and sensitive areas, etc. Despite this, it is certain that the State attaches great attention and importance to the surrounding data collected by vehicle cameras, radars, lidars, and other sensors and such data is to be processed with great care.

Data processing purposes and principles

According to Article 4 of the Draft Provisions, purposes of PI and important data processing are to be legitimate, specific, clear, and directly related to vehicle design, manufacture, and services. Article 6 would apply to the automobile industry the general principle of data minimization set forth in the Cybersecurity Law and the Personal Information Protection Law (Second Reading Draft) and encourage operators to abide by the following principles during data processing activities: (i) in-vehicle processing, (ii) data anonymization, (iii) minimum retention period, (iv) proper precision and scope, (v) no data collection by default.

These principles are not provided as mandatory obligations. Yet, we reasonably foresee the regulatory authorities issuing future implementing rules that take these principles into account. Among other principles, operators would be encouraged to incorporate the principles of "in-vehicle processing"[4] and "no data collection by default"[5] into the technical planning at an earlier vehicle design and development stages.

[4] Article 6.1 of the Draft Provisions: Principle of in-vehicle processing: there shall be no outward data transmission unless it is in fact necessary.

[5] Article 6.5 of the Draft Provisions: Principle of no data collection by default: unless it is indeed necessary, the default setting of each drive shall be no data collection. The consent by the driver to data collection shall only be valid to the specific drive.

Rules on PI processing

According to Article 9 of the Draft Provisions, operators shall obtain data subjects' consent unless laws and regulations otherwise stipulate. When processing PI, operators shall inform data subjects of the items enumerated under Article 7[6], such as the contact information of the person in charge of handling matters related to users' rights and interests, when the data collection will be initiated and how to stop it, and how to delete the collected data. Where it is not practically feasible to obtain data subjects' consent (e.g., when collecting PI outside of the vehicle), consent is not needed for anonymized or de-sensitized data, e.g., by deleting images that can be used to identify an individual or blurring the human faces in such images.

The Draft Provisions respond to the longstanding dilemma on how to lawfully handle pedestrians' PI. According to Article 9, data anonymization and de-sensitization relieve operators from the onerous and nearly impossible burden of obtaining pedestrians' consent. However, there are still two open points that require clarification: (i) whether the term "de-sensitization" has the same meaning as "anonymization" or instead refers to "de-identification"; (ii) whether only vehicle-end data anonymization and de-sensitization would serve to exempt the consent requirement or server-end anonymization and de-sensitization would also suffice. If only vehicle-end data anonymization and de-sensitization would serve to exempt the consent obligation, then operators would have to ensure strong in-vehicle processing capacities. Otherwise, operators would have to rely on legal bases other than authorization and consent for processing PI, which are to be established by the forthcoming Personal Information Protection Law.

Enhanced protection of sensitive PI

Article 8 of the Draft Provisions set forth enhanced requirements for the processing of sensitive PI. The Draft Provisions do not define sensitive PI in the automobile industry but only name three examples, which are vehicle location, audio and video of the drivers or passengers, and data that could be used to determine illegal driving behaviors. When processing sensitive PI, operators would also need to pay attention to the following requirements in addition to those mentioned above:

- **Purpose**: The purpose of processing sensitive PI shall be limited to direct services to **drivers or passengers**, e.g., improving driving safety, driving assistance, navigation, entertainment, etc.
- **Informed consent**: No sensitive PI is to be collected by default. **Each instance** of collection shall be subject to the **drivers'** consent and such consent shall **no longer be valid** at the end of each drive (e.g., when the driver leaves the driver's seat). Drivers and passengers shall be informed of the ongoing collection of sensitive PI via HMI or voice prompt.
- **Control by individuals**: **Drivers** shall be able to stop the collection at any time in a convenient manner. The **vehicle owners** shall be given access to the collected sensitive PI in a convenient

[6] According to Article 7 of the Draft Provisions, items that shall be informed to the data subjects include: (i) contact information of the person in charge of handling matters related to users' rights and interests, (ii) types of the data being collected, (iii) when the data collection will be initiated and the way to stop it, (iv) the purpose and use case of each type of data, (v) the retention location and period of the data, or the rules on determining the same, (vi) how to delete the data stored within the vehicle and the data already transmitted outwards.

and structured manner. Operators shall delete the data within two weeks upon the **drivers'** requests.

The requirements for sensitive PI processing provided in the Draft Provisions are stricter and more detailed than existing regulations, such as the shorter data deletion period. Some of the aforementioned requirements, such as obtaining consent for each drive, could significantly change existing vehicle settings as well as people's driving behavior. Furthermore, Article 8 could be interpreted such that consent is the only legal basis for processing sensitive PI. This may be problematic if the processing of vehicle locations is required to fulfil operators' legal obligations or to protect drivers' safety in emergencies.

Localization of PI and important data

Article 12 of the Draft Provisions provides that operators shall, **by following applicable laws**, store PI and important data within the territory of China and apply for government security assessment for outbound transfers of such data. This ambiguity on localization of PI could be interpreted in two ways. On one hand, the Draft Provision could *per se* mandate all types of automobile PI be stored within China, considering the high sensitivity of data in the automobile industry. On the other hand, it could also be interpreted that the Draft Provisions would not impose additional data localization obligations other than those proposed in the Personal Information Protection Law (Second Reading Draft), pursuant to which automobile operators would be obligated to store PI in China only if they are deemed operators of critical information infrastructure or PI handlers who process PI exceeding certain volume threshold. As for important data, it is more likely the Draft Provision would *per se* mandate local storage of all important data in the automobile industry, considering that the Data Security Law (Second Reading Draft) would empower CAC to stipulate localization rules for important data together with other State Council departments.

Data access and utilization by third parties

In the event that partners of scientific research and commercial operations need to access or utilize PI and important data stored with China, Article 16 would require operators to (i) take effective measures to ensure data security and prevent data leakage, and (ii) strictly restrict the access and utilization of important data and sensitive PI.

Based on textual interpretation, Article 16 would apply to the "access and utilization" of data by third parties rather than "cross-border transfers of data". Considering the common practice of remote data access and emerging technologies such as privacy computing, it is worth exploring whether the aforementioned requirements and restrictions would apply to cooperations between operators and both domestic and overseas partners.

Obligations to report data processing activities

The Draft Provisions would strengthen obligations for reporting data processing activities in the following situations:

- **Advance reporting of important data processing**: Article 11 would require that, prior to processing important data, operators report to the State cyberspace administrations at provincial

levels and competent departments regarding the data types, volume, scope, retention location and period, use cases, and whether the same is to be provided to third parties. Unlike the filing requirement proposed under Article 15 of *Measures for Administration of Data Security (Draft for Comment)*[7], the Draft Provisions would require operators to predict important data processing activities and report the same in advance.

- **Display the types and scope of data in readable plaintext during random inspections**: According to Article 15 of the Draft Provisions, the State cyberspace administrations, along with relevant departments of the State Council, will conduct random inspections of cross-border transfers of PI and important data. Operators would be required to display the types, scope, and other information in readable plaintext.

- **Annual reporting on data security management**: Operators who process PI relating to **more than 100,000 data subjects** and/or important data would be required to report to the State cyberspace administrations at the provincial level and relevant departments by December 15 of each year regarding their data processing activities[8]. Should there be cross-border data transfers, the operators would also be required to report the circumstances surrounding cross-border data transfers[9], including, *inter alia*, data subjects' complaints and handling of the same.

[7] Article 15 of the Measures for Administration of Data Security (Draft for Comment): A cyberspace operator shall file certain information with the local cyberspace administration with respect to the collection of important data or personal sensitive information for business, and the filing information shall include collection and use rules, purpose, scale, method, scope, type and duration, while excluding data content per se.

[8] According to Article 17 of the Draft Provisions, the following matters shall be included in the annual report: (i) name and contact information of the person in charge of data security and the person in charge of handling the person in charge of handling matters related to users' rights and interests, (ii) types, volume, purpose and necessity of the processed data, (iii) data security protection and management measures including data retention location and period, (iv) situations regarding data sharing with third-parties within China, (v) facts and handling of data security incidents, (vi) user complaints regarding PI and data, and handling of the same, (vii) other data security situations designated by the State cyberspace administrations.

[9] According to Article 18 of the Draft Provisions, the following matters on cross-border data transfer shall be included in the annual report: (i) name and contact information of the data recipient, (ii) types, volume and purposes of the transferred data, (iii) the data retention location abroad, scope and method of data use, (iv) data subjects' complaints concerning cross-border data transfer and handling of the same, (v) other situations concerning cross-border data transfer designated by the State cyberspace administrations.

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
Hong Kong	**Dafei CHEN**	**Attorney-at-law**
	Tel:	+852 2820 5616
	Email:	dafei.chen@hankunlaw.com