PAUL HASTINGS

Stay Current

December 2021

Follow @Paul_Hastings

Continued Development of Data Security and Protection in China – All You Need to Know about China's Latest Data Implementation Rules and the New Data Guidance for the Automotive Industry

By Shaun Wu, Phoebe Yan, Sarah Zhu, Tashi Sun, Zoey Xie, & Fengzhen Yu

Rapidly Changing Landscape in China

The year 2021, which brought quite a few changes and developments in the world of business, is approaching its end. With the raging pandemic and continued restriction on travel, the world has become ever more dependent on internet technology, virtual communications, and digital data. Consequently, the importance of data security and privacy protection has now been widely recognized across the globe. In China, 2021 has seen a string of new laws that drastically reshaped the country's landscape for data security and privacy protection. Specifically, the passage of the Data Security Law ("DSL," effective on Sept. 1, 2021) and the Personal Information Protection Law ("PIPL," effective on Nov. 1, 2021) has drastically altered the landscape of data security and privacy protection in China, and attracted attention from observers. *See* our earlier client alert here.

Although the DSL, PIPL, and other existing laws (*e.g.*, Cybersecurity Law of 2017) formulated the overarching structure for data security and privacy protection in China, they also left certain areas open. These areas were meant to be filled by more comprehensive regulations, local-level guidelines, or industry-level rules. Indeed, during the past few months, multiple government agencies in China have been promulgating such regulations and rules, though many of them have not yet been finalized. Here are some examples.

- On Oct. 29, 2021, the Cyberspace Administration of China (the "CAC") issued the Measures on Data Cross-Border Transfer Security Assessment (*Draft*). Although not finalized, these measures sought to provide more details on the conditions and requirements for data cross-border transfer, including CAC's mandatory security assessment, self-security assessment, and the required components in data transfer agreements. For instance, Article 4 provides the following statutory grounds whereby data processors should apply for mandatory security assessment: transfer of personal information and important data collected and generated by critical information infrastructure operators ("CIIO"); transfer of important data; transfer of personal information by data handlers that process more than 1 million individuals' personal information; and cumulatively transferring personal information of more than 100,000 individuals or sensitive personal information of more than 10,000 individuals, among others.

- On Nov. 14, 2021, the CAC promulgated the Network Data Security Management Regulations (*Draft*). This set of regulations, once finalized, would provide comprehensive guidance on the implementation of DSL and PIPL with respect to "network data"; and Article 13 supplemented a mandatory security assessment requirement for data processors handling more than 1 million individuals to go public *abroad* and for data processors to go public *in Hong Kong* that impact or may impact national security.

- On Nov. 29, 2021, the Shanghai Municipal Government issued the Shanghai Data Regulations (*effective on Jan. 1, 2022*), which is China's first comprehensive local data protection guidance.

Most notably, the CAC, together with four other state-level ministries, jointly issued the "Provisions on Management of Automotive Data Security (for Trial Implementation)" (the "Auto Industry Provisions" or the "Provisions"), which came into effect on Oct. 1, 2021. The Auto Industry Provisions were the first set of industry-focused implementation rules of the DSL and PIPL. An analysis of the Provisions would benefit not only players in the automotive industry who would be directly affected, but also the players in other data-heavy industries.

Highlights of the Auto Industry Provisions

Scope of the Provisions

The Auto Industry Provisions defined some industry-specific concepts like "automotive data" and "automotive data processor," and also elaborated on certain key concepts in DSL and PIPL within the context of the auto industry.

1. **Automotive Data**. The Provisions defined a new type of data—"automotive data," which included personal information data and important data involved in the process of automobile design, production, sales, use, and operation and maintenance, among others.[1]

2. **Automotive Data Processors**. The Provisions applied to a wide range of auto industry players in China, including automobile manufacturers, components and parts suppliers, software suppliers, dealers, maintenance organizations, and mobility service companies.[2] This expansive definition also covered companies that provided ride-hailing and sharing services.

3. **Important Data**. The DSL did not offer a clear definition of "important data," but empowered regional and industry authorities to formulate specific catalogs. Here, the Provisions, for the first time, clearly listed five categories of "important data" in the auto industry, which included geographical information, vehicle flow, personal information involving more than 100,000 subjects, and so on.[3]

4. **Personal Information**. The Provisions' definitions of "personal information" and "sensitive personal information" closely followed the definitions in the PIPL, with some specific examples referencing the automobile industry.[4]

Key Principles in Automotive Data Processing

The Provisions outlined the following four key principles for automotive data processing activities, which contained both elements of data security and privacy protection.[5]

1. Principle of processing data inside vehicles. All automotive data must be processed inside vehicles unless it is absolutely necessary to send it out.

2. Principle of non-collection by default. Unless a driver makes a specific selection otherwise, the default setting should be non-collection each time the driver drives the vehicle.

3. **Principle of proper precision in application**. The coverage and resolution of cameras and radars, among others, should be determined according to the requirements for data accuracy of the functions and services provided.

4. **Principle of desensitization**. Automotive data processors are required to apply anonymization and de-identification during processing, if possible.

Requirements on Processing Personal Information

As with the PIPL, the Provisions followed the same principle of "inform and consent." In furtherance of the notification requirements under the PIPL, the Provisions set out a list of items that an automotive data processor must cover in its notice. Specifically, the automotive data processor should notify individuals of the following information in conspicuous ways (*e.g.*, through user manuals, on-board display panels, voice, or applications related to the use of vehicles):[6]

- The types of personal information being processed, including vehicle trajectory, driving habits, audio, video, images, biometric identification features, etc.;
- The specific circumstances under which all kinds of personal information are collected and the methods and means of terminating the collection;
- Purposes, uses, and methods of processing of personal information;
- Personal information retention location and retention period, or rules for determining the retention location and retention period;
- Methods of reviewing and copying personal information, deleting personal information inside vehicles, and requesting the deletion of the personal information that has been sent out of vehicles; and
- The names and contact information of the contact persons for users' rights and interests.

Requirements on Processing Sensitive Personal Information

With respect to processing of sensitive personal information, the Provisions adopted the same rules in the PIPL—that is, businesses can only process sensitive personal information when there are specific purposes and sufficient necessity, with strict protection measures in place. In the context of the auto industry, the Provisions set out the following specific requirements:[7]

- The purpose of processing sensitive personal information should be to serve the individuals directly, *e.g.*, enhancing driver safety, assisting driving, navigation, etc.;
- Automotive data processors should inform the driver and passengers of the necessity and impact on individuals through the user manual, on-board display panel, voice, and related applications, etc.;
- A separate consent from individuals is required, and the individuals can independently set the period of consent;
- On the premise of ensuring safety, automotive data processors should prompt the status of collection in an appropriate manner to facilitate the termination of collection by individuals; and
- If requested by an individual, the automotive data processor should delete the sensitive personal information within ten working days.

Furthermore, the Provisions required that the automotive data processor should not collect biometric identification features such as fingerprints, voiceprints, human faces, and speech rhythms unless the collection was to enhance driving safety and was sufficiently necessary.

Requirements on Processing Important Data

For businesses collecting or generating important data during their operations in China, the Provisions laid out protective measures that were consistent with the DSL, but with more detailed applications in the automobile industry.

- **Data localization and restrictions on cross-border transfer**. The Provisions required all important data to be stored within China. If it is necessary to provide such important data overseas, the data processor must apply for a mandatory cross-border data transfer security assessment with CAC.[8]

- **Self-risk assessment**. The Provisions required automotive data processors to conduct a risk assessment with respect to its important data processing activities, and to submit a risk assessment report to authorities.[9]

- **Annual reporting obligation**. Prior to Dec. 15 each year, automotive data processors dealing with important data were required to report a comprehensive set of information on its data management status, including the responsible person for data security management, the type, scale, purpose, and necessity of processing automotive data, security protection and management measures, whether data were provided to third parties, etc.[10] If important data processing activities carried out by an automotive data processor involved cross-border data transfer, the above annual report should also include additional information, such as basic information of the overseas data recipient, location, period, scope, and retention method of automotive data abroad, and so on.

Looking Ahead

In light of the passage of Auto Industry Provisions, the Ministry of Industry and Information Technology ("MIIT"), the sectoral regulatory for the automotive industry in China, launched a self-inspection program of automotive data security on Sept. 13, 2021, requiring businesses to conduct self-inspection and report non-compliant issues. With the detailed guidance provided by the Provisions, we expect that the automotive industry will face more scrutiny from the Chinese authorities. Similarly, as more rules and regulations are finalized, they will continue to shed light on how the DSL and PIPL would be implemented in a certain industry, or with respect to a certain issue, *e.g.*, cross-border data transfer.

Looking ahead, we suggest multinational companies take proactive steps to mitigate the compliance risks that they may face in this rapidly changing landscape of data privacy and data security law in China. Here are some measures for consideration:

- Perform a data mapping as soon as possible to understand inventories of data and identify important data, personal information, and sensitive personal information that the company is dealing with.

- Perform a health check throughout the data management flow, covering activities of collection, storage, use, processing, transmission, provision, and disclosure of data.

- Perform a gap analysis of the current data-related policies, both internal and external-facing, against China's new data laws.

- Review and update current data compliance clauses in agreements with data-related suppliers, vendors, and customers to ensure that they are still effective given the recent developments of data laws and regulations.
- Set up a risk assessment procedure for major data processing activities, covering functions such as designing, manufacturing, sales, marketing, legal and compliance, and management.
- Launch an internal working mechanism that covers review of data security/data privacy incidents and preparation of report of data management status.
- Perform trainings on the latest Chinese data regulations to enhance awareness of data compliance.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Beijing

Fengzhen Yu
86.10.8567.5358
fengzhenyu@paulhastings.com

Hong Kong

Shaun Wu
852.2867.9088
shaunwu@paulhastings.com

Sarah Zhu
852.2867.9018
sarahzhu@paulhastings.com

Shanghai

Phoebe Yan
86.21.6103.2939
phoebeyan@paulhastings.com

[1] *See* Auto Industry Provisions, Article 3.

[2] *See id*.

[3] *See id*. Specifically, the list of "important data" included (i) Data from important sensitive areas, *i.e.*, military management zones, national defense science and industry entities, and Party and government offices (at least county level); (ii) Data reflecting economic operations, such as vehicle flow and logistics; (iii) Operating data of vehicle charging networks; (iv) Video and image data outside vehicles, *e.g.*, facial information, license plate information, etc.; and (v) Personal information involving more than 100,000 personal information subjects. *Id.*

[4] *See id*. "Personal Information" under the Provisions referred to all kinds of electronic or otherwise recorded information related to the identified or identifiable vehicle owners, drivers, passengers and persons outside vehicles, etc., not including information that has been anonymized. "Sensitive Personal Information" was defined as personal information, of which leakage or unlawful use may lead to discriminatory treatment or serious damage to personal or property safety of vehicle owners, drivers, passengers and persons outside the vehicle, including vehicle location tracking, audio, video, image and biometric characteristics. *Id.*

[5] *See* Auto Industry Provisions, Article 6.

[6] *See* Provisions, Article 7.

[7] *See* Provisions, Article 9.

[8] *See* Provisions, Article 11.

[9] *See* Provisions, Article 10. A risk assessment report should include (i) the type, quantity, scope, retention location and period, and method of use of the important data; (ii) the status of data processing activities; (iii) whether data is provided to a third party; and (iv) data security risks faced and countermeasures. *Id.*

[10] *See* Provisions, Article 13. Specifically, the annual report should include (i) names and contact information of the person in charge of automotive data security management and the contact person for affairs relating to users' rights and interests; (ii) type, scale, purpose, and necessity of automotive data processed; (iii) security protection and management measures for automotive data, including retention location and period, among others; (iv) provision of automotive data to domestic third parties; (v) automotive data security incidents and the handling thereof; (vi) user complaints related to automobile data and the handling thereof; (vii) other automobile data security management information specified by the national cyberspace administration in conjunction with the industry and information technology, public security, transport, and other relevant departments of the State Council. *Id.*