CHINA ISSUES NEW RULES ON DATA SECURITY IN AUTO INDUSTRY

金杜律师事务所
KING&WOOD MALLESONS

How the new regulations will affect auto data in China

by Mark Schaub, Atticus Zhao, Mark Fu

The manner in which China will regulate data security in the automotive industry has become much clearer.

On 20 August 2021, the Cyberspace Administration of China (the "**CAC**"), together with the National Development and Reform Commission, the Ministry of Industry and Information Technology (MIIT), the Ministry of Public Security, and the Ministry of Transport, jointly issued the *Provisions on Management of Automotive Data Security (Trial)* ("**Management Provisions**"), which will take effect on 1 October 2021.

The Management Provisions have made a number of changes to the previously circulated *Provisions on the Management of Automotive Data Security (Draft)* (the "**Draft**") which were issued by CAC in May 2021 for public comments. However, one thing that did not change is China's clear intent that data security of the automotive industry will be strictly regulated.

The main update is that the Management Provisions adopt more accurate definitions and terms, and form a clearer framework regarding the protection and regulating of personal information and important data. Also it can be noted that the legislators have taken pains to have the Management Provisions be consistent with other laws such as Data Security Law .

This article highlights the key changes made in the Management Provisions:

Got questions about this article?
We're happy to talk!
Email mark.schaub@eu.kwm.com, atticus.zhao@cn.kwm.com, and fuguangrui@cn.kwm.com for more information.

1. Scope of Application

The Draft provided a broad definition of “operators” and the data processing activities of such operators were subject to regulation by the Draft. The Management Provisions replace the concept of “operators” with “auto data processor”. The new definition is more appropriate and relevant in the context of data security and consistent with the term “processors” as used in the Data Security Law.

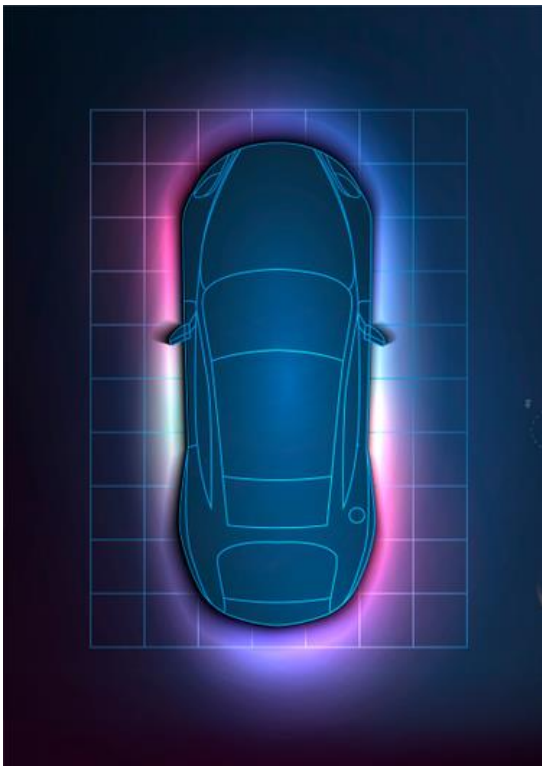
Compared to the previous definition of operators in the Draft, the definition of auto data processor - while still not exhaustive - has a slightly-narrowed scope and refers to organizations that carry out auto data processing activities, including automotive manufacturers, parts and software suppliers, dealers, maintenance organizations, mobility companies etc.

The Management Provisions define “auto data” as personal information and important data involved in the process of automotive design, production, sales, use, operation and maintenance etc.

In the Management Provisions, "auto data processing" includes the collection, storage, use, processing, transmission, provision and disclosure of auto data. All these activities will fall within the ambit of the Management Provisions.

2. Personal Information

One of the most notable changes in the Management Provisions are the provisions relating to personal information. These have been amended to largely align with the Personal Information Protection Law (PIPL) - China's first law solely dedicated to the protection of personal information which was passed on August 20, 2021.



The Management Provisions take the same approach in defining personal information and sensitive personal information as the PIPL, with an application specifically to the auto sector. Under the Management Provisions, personal information is broadly defined as "all kinds of information, recorded by electronic or other means, related to identified or identifiable vehicle owners, drivers, passengers, individuals outside vehicles, etc. not including information after anonymization handling".

The Management Provisions define sensitive personal information as "personal information that, once leaked or illegally used, may easily cause harm to the dignity of vehicle owners, drivers, passengers, individuals outside vehicles grave harm to personal or property security, including vehicle location tracking, audio, video, image and biometric characteristics."

The importance of the distinction between sensitive personal information and "general" personal information is that the conditions to be satisfied for processing sensitive personal information are much higher and stricter.

3. Scope of Important Data

The scope of "important data" defined in the Draft has sparked intense discussions in the market as any data falling within the scope of important data will be subject to stricter regulation.

The Management Provisions change the scope of important data to include:

a) "data on vehicle types and vehicle flows on roads" is replaced with "data such as vehicle flow and logistics that reflects economic operation".

b) "personal information involving more than 100,000 personal information subjects".

c) other data determined by relevant departments that may endanger national security, public interests, or the legitimate rights and interests of individuals or organizations.

The change as described in item (a) above raises the bar for vehicle flow and logistics data that will constitute important data to avoid triggering unnecessary scrutiny at a low threshold.

The inclusion of item (b) above gives a clear guidance to auto data processors the quantity threshold of personal information involved that will constitute important data.

The catch-all clause in item (c) above provides much room for other data to be included as important data.

Another notable change is that the "surveying and mapping data with a level of precision that is higher than maps publicly disseminated by the State" has been removed. It should be noted that the removal of the surveying and mapping data does not mean mapping and surveying data is less important or does not fall within the concept of "important data" but rather that this kind of data will be regulated separately by a different catalogue of important data based on industrial classification given the sensitive nature of surveying and mapping data.

In the Management Provisions, video and image data outside the car including facial information and license plate information remains within the scope of important data.

4. Advocative Principles in Data Processing

The Management Provisions largely retain the “advocative principles” for the process of auto data as previously introduced in the Draft. Specifically, the Management Provisions advocate the principles of “in-car processing”, “no collection by default", “proper precision” as well as “anonymization” in processing auto data. Specific issues include:

a) **In-car processing:** auto data should be processed inside the vehicle, unless there is a sufficient necessity to provide the data outside of vehicles.

b) **No collection by default:** the default setting should be that there is no collection of auto data unless the driver specifically sets otherwise. The previous Draft provided that the drivers’ consent is only for a single drive, but the Management Provisions have provided more flexibility by allowing drivers to set the collection of auto data without specifically limiting on the frequency.

c) **Proper precision:** data processors shall determine the coverage and resolution of cameras, radars, etc. based on the data accuracy requirements of functional services provided; and

d) **Anonymization:** data processors should conduct de-identification and anonymization of auto data to the greatest possible extent. In the previous Draft, the principle was set with the “in-car processing principle”, under which information must be anonymized and de-identified to the greatest possible extent before being provided outside vehicles. The Management Provisions, have tweaked this principle by providing a broader application on all aspects relating the process of auto data, including using and storage of auto data. Furthermore, de-identification and anonymization are specifically defined terms under the PIPL: “de-identification” refers to the process by which personal information is handled so as to ensure it is impossible to identify specific natural persons without additional information being provided. On the other hand “anonymization” refers to the process by which personal information is handled so as to make it impossible to identify a specific natural person and which is also impossible to restore.

Another important change is that, the Management Provisions have deleted the fifth principle originally set out in the Draft – namely, the minimum retention period principle. The previous Draft had provided that retention period be determined based on the category of function and service.

4. Advocative Principles in Data Processing (cont.)

However, we do not believe that the deletion of such minimum retention period principle in the Management Provisions does not mean it is no longer applicable. Rather, the legislation is better joined up and it is now explicitly provided in the PIPL, that a mandatory requirement for all sectors, that personal information retention periods shall be the shortest period necessary to realize the purpose of the personal information handling unless otherwise provided for by law.

The foregoing principles have raised some discussions in the Draft as “advocative principles”– the consequence for non-compliance of such advocative principles is not mandatory and therefore are not of legally binding effect. However, we suggest companies taking a wait-and-see approach on the principles, as there has been a trend that such advocative principles, especially those in cybersecurity regime, are likely to be so influential that they become the basis for non-compliance remediation plans and undertakings agreed between companies and regulators.

For this reason, companies are suggested to adopt advocative principles to the extent practical in order to show their compliance efforts in China meet the necessary benchmarks.

5. Statutory Requirements for Processing Personal Information

The Management Provisions made slight revisions to the previous Draft in relation to the statutory requirements for personal information processing.

1. Processing Personal Information

When processing personal information, the data processor is required to inform the types of data being collected and provide the contact information for the responsible person. The notice can be provided through user manuals, onboard display panels, or other appropriate methods.

The notice should also include the scenarios for collection of personal information and how to stop the collection, the purpose and usage for collection, where and for how long data is stored or rules for determining the retention place and period, how users can access, copy and delete data stored in the car or provided outside the vehicle.

5. Statutory Requirements for Processing Personal Information (cont.)

2. Processing Sensitive Personal Information

The Management Provisions set out the following requirements for data processors to process sensitive personal information:

a) serve the individuals directly, for example, enhancing driver safety, assisting driving, navigation, etc.

b) 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.;

c) obtain separate consent from individuals, where the individuals are allowed to set the time limit for such consent independently;

d) under the premise of ensuring driving safety, remind the collection status in an appropriate manner, and allow individuals to terminate the collection conveniently;

e) if requested by an individual, the auto data processor shall delete the sensitive personal information within ten working days.

For item (a) above, compared with the Draft, the Management Provisions removed entertainment as processing sensitive personal information. Companies should be more cautious as to collect or otherwise use sensitive personal information for entertainment before greater clarity is available.

Furthermore, the Management Provisions single out the conditions for collection of biometric data such as fingerprints, voice prints, faces and heart rhythms – the foregoing biometric data may be collected only if (i) the purpose is for enhancing driving safety and (ii) there is a sufficient necessity.

As mentioned above, the conditions set here for processing sensitive personal information are consistent with those already provided for in the PIPL – namely, only where there is a specific purpose and sufficient necessity can sensitive personal information be processed. Also even in such cases the processing must comply with strict protection measures. The Management Provisions also request Auto data processor to inform the necessity and the impact on individuals, and powers the individuals the rights to set the period of consent and deletion. The Management Provisions have removed the highly debated “single consent requirement” as previously provided in the Draft, where a consent is required every single drive when collecting sensitive personal data.

6. Exception for Consent from Individuals Outside Vehicles

In contrast with the Draft, the Management Provisions keep the exception for consent from individuals outside vehicles but narrow down the applicable conditions as follows:

a) solely for ensuring driving safety, and

b) personal information of individuals outside vehicles should be anonymized – all images by which individuals may become identifiable or with individual faces should be either anonymized or desensitized.

This exception for the general principle of obtaining consent before collection and provision of personal information only applies to personal information of individuals outside vehicles. The triggering event is strictly defined – it will not work for personal information of vehicle owners, drivers or passengers, nor would it apply to collection of personal data for individuals outside vehicles for any purposes other than ensuring driving safety.

7. Important Data Risk Assessment Report

In the Draft, an operator is required to report to competent authorities in advance when handling important data. This requirement is inconsistent with that of under the Data Security Law. Article 30 of the Data Security Law provides that "processors of important data shall conduct risk assessments of their data processing activities on a regular basis in accordance with the provisions and submit risk assessment reports to the relevant competent authorities. The risk assessment report shall include the type and quantity of important data processed, the state of data processing activities, the data security risks and the measures to address them, etc."

In order to be consistent with the Data Security Law, the Management Provisions adopt similar language in this regard. However, the Management Provisions have not specified when the risk assessment report should be submitted to the authorities. The Data Security Law requires that such risk assessment be made “on a regular basis” and submitted to authorities. The implementation details for the Management Provisions will need to be further clarified by authorities.

8. Data Localization and Cross-border Transmission Requirements

The Management Provisions made no changes on the localization requirements as to important data, i.e., important data must be stored in the country as required by law, and security assessments shall be made with the CAC and other governmental authorities if cross-border transfer is needed.

The Management Provisions also stress that vehicle data processors who provide important data overseas must not exceed the purpose, scope, method, type and scale of the data specified in the security assessment, and that the auto data processor shall cooperate and display the important data transferred offshore in a readable and other convenient manner when CAC and other departments make checks.

On 12 August 2021, the MIIT released the Opinions on Strengthening the Management of Intelligent and Connected Automotive Manufacturers and Product Access (the "MIIT Opinions"), which requires smart car manufacturers to store personal information and important data in country, and security assessment needs to be made in case of cross-border transfer of personal data and important data.

It is clear the MIIT Opinions set stricter requirements for smart car manufacturers as both personal information and important data are required to be stored "in country". In this regard, smart car manufacturers appear to fall within the ambit of being deemed as critical infrastructure information operators (CIIO). For a CIIO, both personal information and important data must be stored in country in accordance with the China Cybersecurity Law.

Another important change is that the Draft imposed restrictions on data sharing and commercial use by requiring that where scientific research and commercial partners need to inquire and use personal information and important data stored within the PRC, operators should take effective measures to ensure data security and prevent loss of data, and that operators shall strictly limit the use of important data. This restriction was seen by many as a prominent obstacle for the reasonable commercial flow of auto data.

The said restrictions have been removed in the Management Provisions. The Management Provisions stress that one of the purpose of the Management Provisions is to promote reasonable development and utilization of auto data.

金杜律师事务所
KING&WOOD
MALLESONS

9. Annual Reporting Requirements

The Management Provisions largely keep the same annual reporting requirements as specified in the Draft.

According to the Management Provisions, the auto data processor must report on various information to the authorities including the activities that provide important data to a third party in China and auto data security incidents and the handling of such incidents. Those involving cross-border data transmission are additionally required to report the basic information of the data receiver, as well as the location, scope, term and manner of use of storage outside the country.

金杜律师事务所
KING&WOOD MALLESONS

Suggestions

China has established its main legal regime in regulating cybersecurity, data security and personal information protection with the promulgation of Cybersecurity Law, the Data Security Law and PIPL.

Smart cars will be collecting, processing and transferring data at levels previously undreamt of. However, such activities will prove to be a great challenge to the Chinese regulators. Following the effectiveness of the Data Security Law, the PIPL and the Management Provisions, we expect to see enforcement against some major players to make it clear that China will enforce data security and personal information protection.

Companies that will be affected should consider the following:

1. Consider data security issues in the process of designing, producing, selling, operating, maintaining and managing cars, and reduce the amount of data collected and stored in car to the greatest possible extent.
2. While using big data for commercial operations, safeguard the users' right to know and implement technical safeguards to desensitize and anonymise data, as well as preventing misuse or unauthorized third-party access.
3. Multinational companies or Chinese companies with R&D centres outside China should consider implementing localized storage as soon as possible by establishing data centres within China and enhancing local R&D capabilities in China.
4. Finally, companies would be well advised to conduct a systematic review and assessment of the current state of their data handling. Business operations that clearly do not comply with the requirements of the Management Provisions should be adjusted in a timely manner.

About the authors

Mark Schaub

Managing Partner
London, Shanghai, Frankfurt
mark.schaub@eu.kwm.com

Atticus Zhao

Partner
Shanghai
atticus.zhao@cn.kwm.com

Mark Fu

Partner
Shanghai
fuguangrui@cn.kwm.com