DS NEWSLETTER savoir, faire
NEWSLETTER – LEGAL INFORMATIONS
PROPOSED BY DS AVOCATS

What to know about data of connected vehicles? ASIE

BACKGROUND

Obviously, 2021 is an important year for data protection in China. With the entry into force of *PRC Civil Code* at the beginning of this year, in the second half, *Data Security Law* (***"DSL"***) and *Personal Information Protection Law* (***" PIPL"***) were successively promulgated. Thus, the legal framework for data protection in China is basically formed.

Simultaneously, in recent years, with the trend of data protection and the development of automotive industry, regulation and national standard related to intelligent connected vehicles (***"ICV"***) have also been released one after another. On the one hand, China encourages and promotes the development of automotive industry and the utilization of transportation big data. On the other hand, until recently the special legislation of vehicle data supervision was almost absent.

Eventually, the *Regulation on Vehicle data Security Management (for Trial Implementation)* (***"Regulation"***) was issued on August 16th, 2021 and came into force on October 1st, 2021.

IMPORTANT CONCEPTS

Although with *DSL* and *PIPL* in place to define some basic data concepts, the *Regulation* re-defines some similar concepts by giving them automotive features as the underlined parts show.

	Definition
Vehicle data	includes personal information and important data involved in the process such as the design, manufacturing, sale, use, operation or maintenance of vehicles.
Processing of vehicle data	includes the collection, storage, use, processing, transmission, provision, and disclosure of vehicle data.
Vehicle data processor	refers to organizations that carry out any activity processing vehicle data, including automotive manufacturers, parts and software suppliers, dealers, and repair and maintenance service providers, car-booking service companies etc.
Personal information	refers to any type of information related to an identified or identifiable vehicle owner, driver or passenger or any person outside the vehicle that is electronically or otherwise recorded, excluding information that has been anonymized.
Sensitive personal information	refers to any personal information that, once leaked or illegally used, may lead to discrimination against or grave harm to personal or property safety of a vehicle owner, driver or passenger or any person outside the vehicle, including vehicle location tracking data, audio, video, image, biometrics and other information.

Furthermore, the *Regulation* also mentions five types of data considered as important data. According to *Cyber Security Law* ("***CSL***") and also the *Regulation,* important data shall be stored in China, and any cross-border transfer are subject to security assessment conducted by competent authorities.

No.	Scopes of important data specified by the *Regulation*
1	Geographical information, flows of people or vehicles, and other data in respect of any important sensitive area such as a military administrative zone, national defense science and technology development entity, or Party or government agency;
2	Traffic volume, logistics and other data that reflect performance of the economy;
3	Operating data of a vehicle collected by the network used for charging;
4	Video or image data collected outside of a vehicle including individual facial information, license plate information, etc.;
5	Personal information involving more than 100,000 individuals;
6	Other types of data which competent authorities consider as capable of endangerment of national security or public interests, or infringement of the lawful rights and interests of an individual or organization, once such data is leaked.

It is noteworthy that personal information can be considered as important data in the context of automotive industries when it is related to sensitive data (facial information) or reaches a certain amount (100,000 individuals).

PRINCIPLES OF VEHICLE DATA PROCESSING

Besides the minimization and necessity principle of data processing, and the Multi-Level Protection Scheme ("***MLPS***") required by *CSL*, the *Regulation* puts forward additional requirements for the processing of vehicle data:

1) The principle of in-vehicle processing. Out-of-vehicle processing can only be conducted unless it is necessary to provide data to a recipient outside the vehicle.
2) The principle of non-collection by default. It means that the default setting should be "no collection of data" in every trip unless the driver sets it otherwise as decided by him/her independently;
3) The principle of appropriate accuracy and coverage. It means that the range of coverage and resolution of any camera, radar etc. are determined based on the requirements for data accuracy by the provided functions or services; and,
4) The principle of desensitization. It means that data is anonymized or de-identified as best as possible.

To ensure driving safety, personal information of individual outside the vehicle could be collected during driving. In this scenario, the *Regulation* also specifies that if these personal information cannot be collected with consent of the individual, the collected personal information shall be anonymized, including deleting the picture containing natural persons, or perform local contour processing on the facial information in the picture.

If personal sensitive information is involved, the vehicle data processor shall obtain the separate consent of the data subject. The vehicle data processor can only collect biometric information such as fingerprint, voiceprint, facial information, heart rate and so on when he/she has the purpose of driving safety and sufficient necessity. If a data subject requests deletion, the vehicle data processor shall delete it within 10 working days.

SUPERVISION OF DATA PROCESSORS AND CROSS-BORDER DATA TRANSFER

In addition to the local storage and cross-border transfer assessment required by *CSL* for important data, the *Regulation* sets forth that for ICV related enterprises who process important data:

1) To submit safety management information to the regulatory authority every year. The submitted information includes: the person in charge of vehicle data safety management, type of data, volume of data , safety protection measures, domestically shared data, disposal of safety events, and handling of complaints from relevant users;

2) As for cross-border data transfer, besides the above, to additionally submit: basic information of data recipients; type, volume, purpose and necessity of data transferred; the storage location, retention period, scope and method of vehicle data storage; handling of user complaints involved in transferring vehicle data overseas.

**It is recommended that ICV related enterprises pay attention to whether their industry has a requirement of a minimum retention period of data. For example, for online car-booking platform companies, the personal information collected and the business data generated shall be stored and used in mainland China, and the retention period shall not be less than 2 years.*

OTHER LEGAL UPDATES OF ICVS

1) National Policies

It is worth mentioning that before the *Regulation* came into force, the *Ministry of Industry and Information Technology* ("***MIIT***") issued the following two important policies on ICV. They show that ICVs are gradually required to be "safe by design" in terms of vehicle data and other aspects.

- *The Opinion of the MIIT on Strengthening the Administration of the Access of ICV Manufacturers and Products* effective on July 30th, 2021.
- *The Circular of the MIIT on Strengthening the Cyber Security and Data Security of the Internet of Vehicles* effective on September 15th, 2021.

2) National Standards

The compliance requirements for vehicle data in the *Regulation* may be too broad and vague, but there are already some drafts of national standards related to vehicle data, which may shed some lights on "how to do vehicle data compliance" for enterprises.

Per two recent national standards, *Information Security Technology - Guide for Data Security of Online Car-Booking Services* (*Draft for Comment*), and *Information Security Technology - Security Requirements for Data Collected by Networked Vehicles* (*Draft for Comments*), trip track and trip recording data are not recommended to be stored in the office terminal but in the server with security protective measures, and some vehicle data (i.e. road, building, terrain, traffic participants and other data collected by ICV from the external environment) should not be transmitted to overseas.

**Please note that the above national standards are still in the draft status at the time of publication of this article.*

COMMENTS

Due to the characteristics of vehicle data, we suggest that relevant ICV enterprises conduct self-assessment on their compliance according to the existing basic *CSL*, *DSL*, *PIPL*, and other industry regulations (such as the *Regulation*), national standards, etc. If there are any imperfection, it is necessary to form a professional team and start the compliance project as soon as possible.

According to the *Regulation*, the processor of vehicle data is likely to face a collaborative supervision of multiple regulatory authorities, including but not limited to China Information Office, the Ministry of Development and Reform, MIIT, the Ministry of Public Security, the Ministry of Transport, etc. In order to cope with the dynamic supervision from authorities, we suggest that in practice, ICV relevant enterprises pay more attention to the notices and updates released by various regulatory authorities, so as to maintain initiative in compliance work.

For any additional information please contact:

ZHANG Beibei
Associate - Shanghai Office
beibeiZHANG@dsavocats.com

Isabelle DOYON
Lawyer- Shanghai Office
DOYON@dsavocats.com