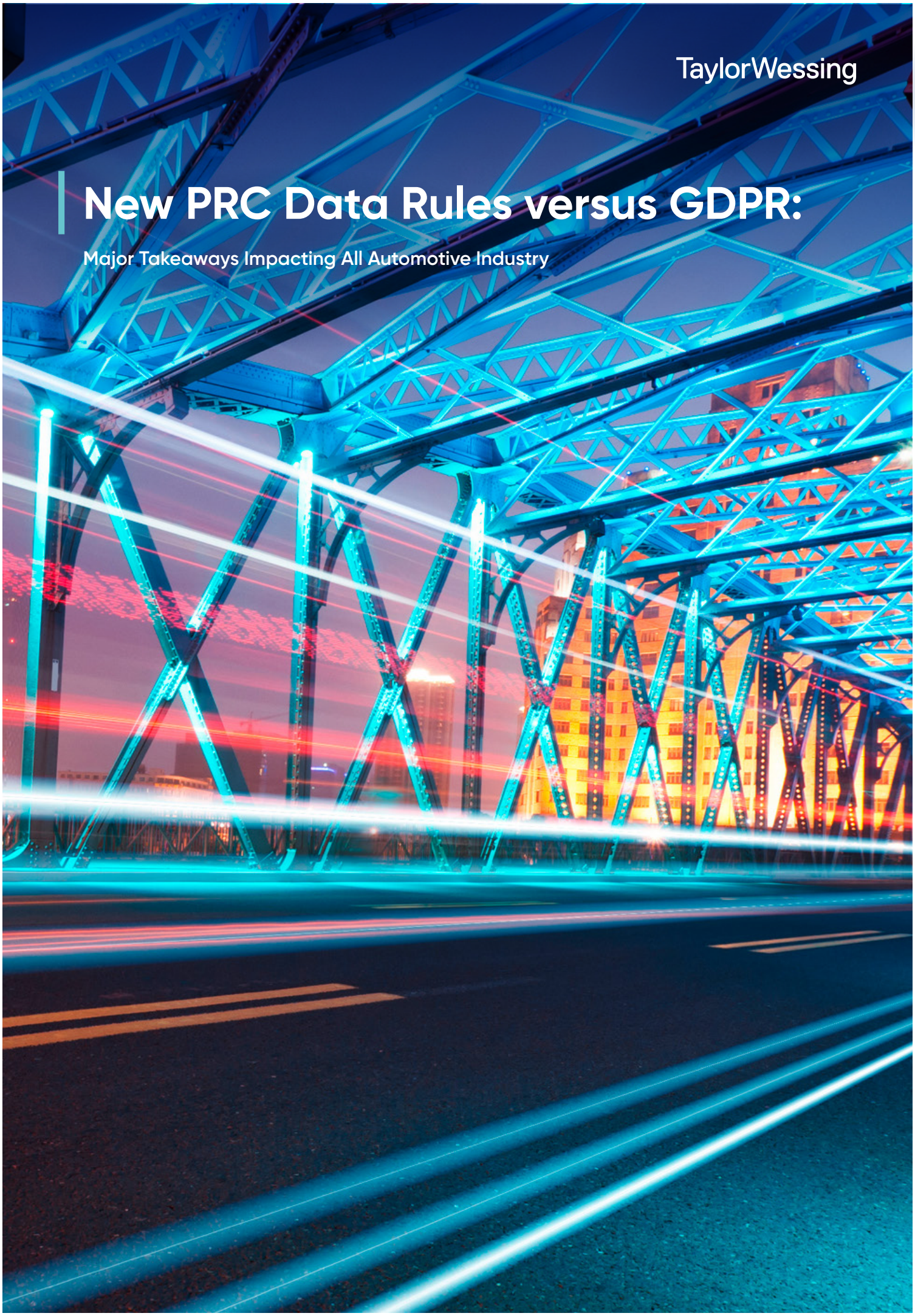
TaylorWessing

New PRC Data Rules versus GDPR:

Major Takeaways Impacting All Automotive Industry



International automotive OEMs and suppliers have witnessed the rapid development of the PRC data protection regime, including the draft *PRC Personal Information Protection Law* which just underwent its "second reading". While existing rules only generally address concerns relating to privacy protection and data export control, rules specific to the automobile industry have been absent for a long time. This makes it difficult for the automotive industry to manage their data compliance in China. Such situation may soon change, as the Cyberspace Administration of China (CAC) presented to the public its new draft *Several Provisions on Car Data Security Administration* on May 12, 2021 (**"Draft Provisions"**) to solicit comments.

The Draft Provisions, if promulgated in the current form, would on the one hand bring substantial clarification to the whole industry, though not make things easier.

On the other hand, the new developments are forcing manufacturers to measure their concepts developed under the strict requirements of the GDPR and the guidelines issued by the European data protection supervisory authorities (find the most current version of the European Data Protection Board's Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, the **„Guidelines"**, here) against the requirements of proposed Chinese law. This will be of particular importance where manufacturers will aim at developing and marketing their technologies in a variety of markets with uniform configurations which will be made more difficult where deviating requirements and standards exist in different parts of the world.

Please find below brief observations and thoughts of our data protection and China experts comparing the Draft Provisions to the concepts and major views of European data protection authorities on the handling of (personal) data from the connected vehicle landscape under the GDPR.

Content

The core team

Dr. Michael Tan
Partner
+86 21 6247 7247
m.tan@taylorwessing.com

Thomas Kahl
Partner
+49 69 97130 0
t.kahl@taylorwessing.com

Scope – What's regulated by law?

Car Data Security Regulation for China – Wide Coverage involving Everyone and Everything

By using the very broad term "operator", the Draft Provisions would apply to almost all members of the automotive supply chain including OEMs, components and software suppliers, dealers, repair shops, online car-hailing service providers, and insurance companies.

As far as personal information or so called "important data" are concerned, all data activities such as collection, analysis, storage, transmission, searching, use, deletion and export would be captured.

Notably the Draft Provisions expand the scope of personal information from "inside a car" (i.e. information of car owners, drivers, passengers) to "outside a car" (i.e. information of pedestrians, etc.) as well as to other information that can be used to identify an individual or that describes personal activities. The "important data" is further clarified by the Draft Provision and would include:

(i) traffic data in important and sensitive areas (e.g. military zones and defense/science units which involve state secrets, governmental/CPC agencies above county level);

(ii) mapping and surveying data more precise than maps published by the State;

(iii) operational data of car charging station/networks;

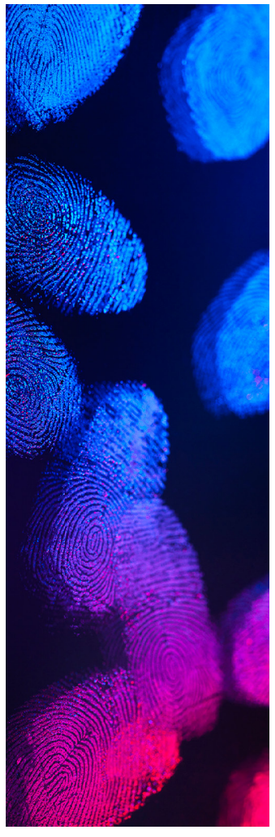
(iv) data on vehicle types and flows on roads;

(v) outside-a-car audio and video data that contain information on e.g. faces, voices, car plates; and

(vi) other data that concern national security and public interest as classified by the CAC and other ministries.

Under the Draft Provisions, an operator shall process the above data for purposes directly relating to the design, manufacturing and service of cars only and shall comply with cyber security requirements, including to implement the latest multiple level protection scheme (MLPS).

The emphasis on the "important data" (which will be associated with further legal obligations, see below) would create a unique challenge for global players in the auto industry.



GDPR – Limited scope for personal car data, but very complex legal landscape

The handling of vehicle data has so far been regulated only partially and in a fragmented manner in European law. A regulation comparable to the Draft Provisions, in which other data law driven aspects (other than the protection of personal data) are addressed, is currently lacking in European law.

At the level of European law, on the one hand, the requirements of the GDPR impose considerable restrictions on the processing of vehicle data or data obtained in the vicinity of the vehicle by means of cameras or other sensors (environmental data), insofar as this is personal or identifiable data.

The scope of application of the GDPR and related national data protection laws is thus much narrower than that of the current Draft Provisions under the Chinese court, some of which also include non-personal data in the scope of regulation.

The requirements of the GDPR, which are generally technology-neutral and rather non-specific, were most recently concretized with regard to the handling of vehicle data by the EDPB's Guidelines (an overview of the main findings and major take aways for automotive companies can be found **here**).

In some cases, isolated regulations on the handling of personal vehicle data can be found in national laws regulating the implementation of automated or autonomous vehicle technologies in the respective national road traffic laws.

Further regulations on the handling of (non-personal) data obtained in the environment of connected vehicles can also be found in various other regulations at the level of European law, including REGULATION (EU) 2018/858 on the approval and market surveillance of motor vehicles incl. the requirements on cyber security and cyber security management system of the UN.ECE WP 29 working group, which have been implemented in European law since mid-2020, or the EU Regulation No. 2019/2144 on the mandatory implementation of measures to protect traffic by means of assistance systems by June 2022.

As a major take away it can be stated that the Draft Provisons take a different approach than current EU laws. The data protection requirements of EU law have a much narrower scope of application. In addition, EU law contains complex and highly fragmented regulations on individual aspects of handling vehicle data, which are difficult to penetrate without special knowledge of the regulatory system.

The differences between the respective legal systems will pose challenges for manufacturers, as a comparison of the existing regulations under EU law and Chinese law on how to treat car data is not a simple "tick-the-box" exercise, but requires a more intensive examination of the individual legal requirements.

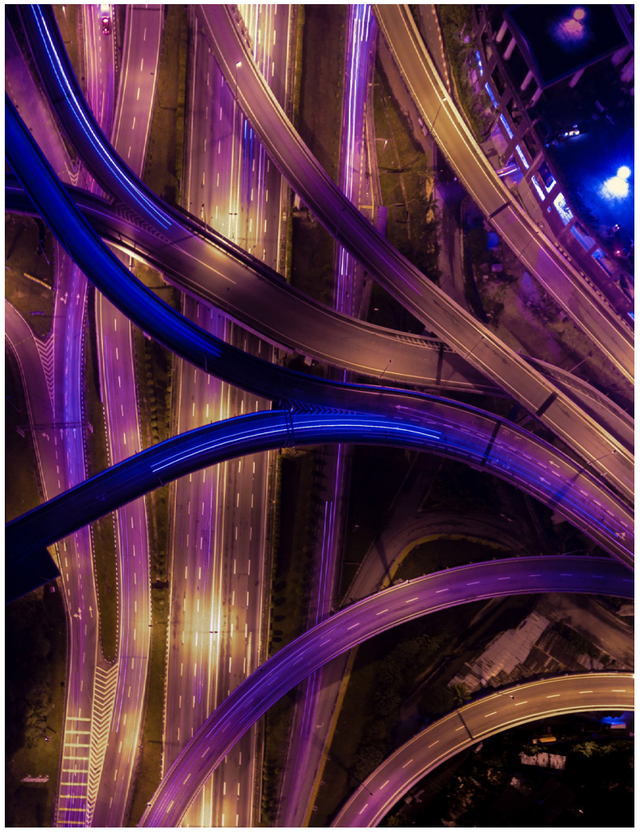
Data Processing Principles for car data

New Car data processing principles under Chinese Law – In-car Requirement by Default

OEMs and data-rich suppliers would need to pay particular attention to the following data processing principles introduced by the Draft Provisions:

- **(i)** in-car processing:
  data shall be processed "in a car" instead of "out of a car" in principle;
- **(ii)** anonymized processing:
  if it is indeed necessary to provide data out of a car, such data shall be anonymized and desensitized;
- **(iii)** minimum retention period:
  data retention period shall be determined according to the type of services/functions offered;
- **(iv)** precision as necessary:
  coverage and resolution of sensors like cameras and radars shall accord to the precision demanded by the offered services; and
- **(v)** "non-collection" by default:
  by default, no data shall be collected for each drive, and a driver's consent shall only apply to one single drive.

The Draft Provisions take a "processing in car by default" approach, which weighs privacy over the commercial and operational features of a "connected car".



GDPR requires similar approaches – but maybe even less strict?

Similar to the Draft Provisions GDPR sets data minmization as a core requirement of European data protection law (see Article 5 (1) of the GDPR). And in its current guidelines, the EDPB also follows the principle of "processing in car by default" as provided for in the Draft Provisions and is very similar to the requirements in this respect. Thus, also under GDPR data processing inside and outside the vehicle should already be minimized as much as possible, among other things by implementing suitable technologies (e.g. anonymization of data, short storage periods for data, etc.).

Both, the Draft Provisions and GDPR as concretized by the EDPB's Guidelines jus recently seem to award a major role to user consent as likely the essential legal justification for processing personal vehicle data in the connected vehicles ecosystem under the GDPR. While this classification is controversially discussed under EU laws it will continue to pose significant challenges for manufacturers when handling vehicle data. For example, under the GDPR the corresponding approach of the EDPB is likely to make a meaningful balance between the various obligations in the area of IT security, product monitoring or quality management and the strict requirements postulated by EDPB, while not impossible, considerably more difficult. It is to be seen how the new rules will be interpreted and executed by Chinese authorities once in effect but the Draft Provisions show a similar understanding on the dealing with (personal) car data as it is currently emphazised by the EDPB under GDPR.

So, looking at both, GDPR and the Chinese Draft provisions and the principles contemplated by them, European manufacturers should be quite well prepared for the Chinese market and the future requirements there when following the strict requirements of the EDPB in its current Guidelines, which appear to be at least very similar.

However, as we will see in the following, the Chinese Draft Provisions come up with several "surprises", one of them being the requirement that the user's consent can only be given per trip and then automatically loses its effectiveness. This concept is likely to "exceed" the requirements of the GDPR at first glance. Thus, under the GDPR, constellations seem quite conceivable in which - in accordance with the GDPR - technology settings in the vehicle are determined by the user permanently or at least for a certain period of time. It also seems questionable whether corresponding concepts do justice to the complexity of modern vehicle technologies, especially in the area of assistance systems.

In any case, it remains to be seen whether this particular advance in the "new" Chinese law will result in the emergence of a new "privacy gold standard", which is likely to pose certain challenges in the future for manufacturers who have essentially aligned their technologies with the requirements of the GDPR to date.

Processing of sensitive categories of car data

Chinese law sets strict rules for sensitive processing activities

Processing of sensitive personal data (e.g. vehicle location, audio/video of drivers and passengers, wrongful or illegal driving behavior, etc.) out of a car shall be prohibited, unless:

(i) it is for the purpose of directly serving the driver or passengers, including enhancing driving safety, assisting driving, navigation and entertainment;

(ii) it defaults to "non-collection", and consent from the driver is required for each drive which will automatically become invalid upon end of a drive (i.e. when a driver leaves his/her seat);

(iii) the driver and passengers are informed, via in-car display panel or by voice, that (sensitive) personal information is being collected;

(iv) the driver may stop data collection at any time in a convenient way;

(v) car owner may review in a convenient way or enquire in a structured way the (sensitive) personal information collected; and

(vi) the operator shall be obliged to delete data within two weeks upon request by the driver.

GDPR also extensively regulates the handling of position data, biometric data, and data that provides information about possible violations of the law

The processing of special categories of personal data, namely location data, biometric data and data that provide information about possible misconduct with the law, is also to be possible under the GDPR only in compliance with very restrictive requirements. According to the principles of the GDPR, the consent of the user should always be required for the processing of corresponding data.

At first glance, it appears that Chinese law may become even stricter than the GDPR already is in this particular regard.

First, it is unclear under the Chinese Draft Law whether, and if so to what extent, the processing of sensitive data can be justified by consent if the processing is for purposes other than those specified in the law ("convenient use or for security reasons"). If so, this might materially limit the options for processing activities for manufacturers and service providers if outside of the scope defined by law.

Second, the draft Chinese law emphasizes that consent granted can – again – only remain valid for the specific trip and automatically expires thereafter. As previously addressed, the GDPR is likely to provide greater room for maneuver here if necessary (including in the creation of "profiles" in the vehicle and querying consent when it is first collected) which will pose challenges on EU stakeholders when localizing their concepts to the Chinese market.

Third, the Chinese Draft Law seems to provide for even stricter transparency requirements than GDPR already does. The EDPB also calls for more comprehensive transparency in the processing of personal data in the vehicle. It recommends appropriate notices on data processing to assist the user, e.g., through a clear signal on-board, such as a light inside the vehicle to inform passengers about data collection. In contrast to the Chinese Draft Provisions, which seem to make it mandatory to inform the user via an in-car display panel or by voice, the EDPB's specifications are likely to be understood as a recommendation or indication of possible designs, which should still leave manufacturers a certain amount of freedom.

Finally, the very short deadline for deleting vehicle data of only two weeks under the Chinese Draft Provisions is striking. It is unclear whether this deadline applies only to out-of-car data or also to in-car data.

The approach itself is in line with the thoughts of the EDPB in its current Guidelines. In the Guidelines comprehensive control of the data subject over the in-car and out-of-car data processing activities should be a basic requirement for the implementation of the requirements of the GDPR. The early deletion and anonymization (and pseudonymitzation) of vehicle data (so-called "hybrid processing") as well as the implementation of a profile management system with which the user can control the collection, storage and processing of data in the vehicle in a targeted manner and by simple means are likely to become essential building blocks in any car privacy concept under the GDPR.

However, the Guidelines do not contain any specific deadlines as provided for in the Chinese Draft Provisions, which requires recourse to the general principles of the GDPR, according to which personal data must be deleted as soon as the respective processing purposes no longer apply.

While European law may offer manufacturers and providers a certain degree of flexibility, the rigid deadlines of the Chinese Draft Provisions are likely to pose challenges in the design of corresponding processes, which will require consideration of local requirements.

TaylorWessing

Data Collection

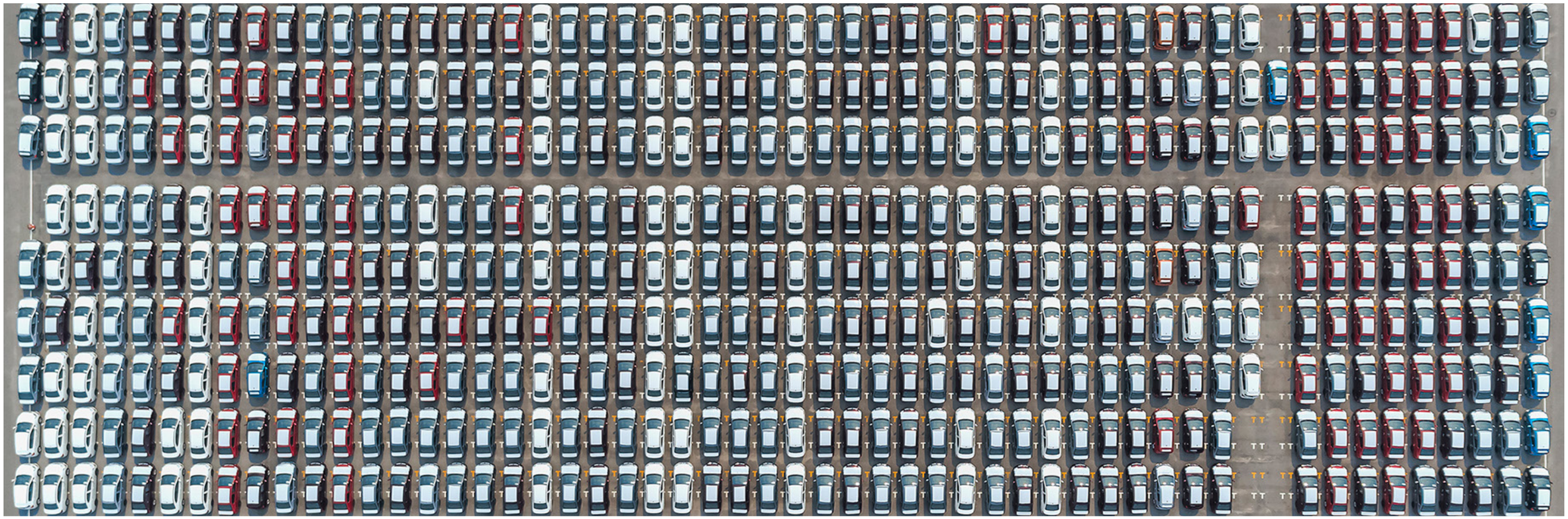
New Transparency principle in the Chinese Law

The general transparency principle on data collection will also be substantiated under the Draft Provisions. An operator would therefore be obliged to disclose a variety of information about the data collection (e.g. type of data collected, method of and purpose for collection, data storage location and retention period, as well as "right to be forgotten"). Collection of biometric data would be allowed only for purpose of convenient use or for security reasons.

GDPR – Transparency remains „key" aspect

As already explained, the EDPB under the GDPR also requires a high degree of transparency in the processing of vehicle data. Users must also be comprehensively informed about the details before the respective data processing begins. In its Guidelines, the EPDB specifies the options for informing data subjects. The data subjects may be informed by concise and easily understandable clauses in the contract of sale of the vehicle, in the contract for the provision of services, and/or in any written medium, by using distinct documents (e.g., the vehicle's maintenance record book or manual) or the on-board computer. In addition, the EDPB emphasizes the use of standardized symbols/icons to facilitate the communication of information.

Having said that, European manufacturers and providers, it remains to be seen how the information obligations under the Chinese Draft Provisions will be concretized in the future - with the exceptions described above - manufacturers seem to be quite well equipped for the future Chinese law with their concepts developed under the GDPR, which should at least to some extent simplify the rollout of internationally uniform concepts.



Reporting Obligations and Data Export

Extensive Obligations and strict requirements under Chinese law

The Draft Provisions set extensive reporting requirements on operators that process "important data" or personal data of more than 100,000 individuals. In reality this would be quite challenging: for example, an operator can hardly prevent a driver from using a smart car in a sensitive area, and the threshold of 100,000 individuals may be easily triggered if an operator engages in public transportation or has high sales of smart cars. The reporting requirements would include that a report on the names and contact details of the data security officer and the person responsible for data issues shall be submitted to the CAC and (other) relevant authorities at the provincial level by December 15 of every year as well as that any processing of "important data" shall be reported beforehand, indicating the type, scale and scope of data, storage location, retention period, method of use, and status of sharing with third parties.

The Draft Provisions further would require (car-related) personal data and "important data" to be stored within the PRC. Any data export (which will technically also include access to data from overseas), if indeed necessary, shall then:

- undergo data export security assessment as organized by the CAC;
- have effective measures in place to regulate export of data and to ensure data security;
- oblige an operator to take care of data subjects' complaints and assume legal liabilities for any damages suffered by the data subjects or damages to "public interest" due to data export; and
- allow the CAC (together with other authorities) to conduct necessary audit by providing plaintext and readable access.

The Draft Provisions specifically address the scenario where an operator's overseas R&D or commercial partner needs to access its data stored onshore. In this case, effective measures shall be taken to ensure data security and prevent data breach, while access to "important data" and sensitive personal data shall be strictly restricted.

European Laws take similar approaches

European data protection law does not contain any corresponding reporting obligations in this form. However, the obligations are very similar to the EU legal requirements of the NIS Directive, which have been implemented in national law in the various EU member states in recent years and are currently being further specified. According to this directive, operators of critical infrastructures are obliged to submit various reports to the relevant supervisory authorities (including in the event of security incidents) and to set up certain internal structures to manage IT security in the company accordingly.

European law does not yet include an explicit obligation for automotive manufacturers and service providers in the automotive sector to submit corresponding reports or meet similar notification obligations, but providers of corresponding services may already be subject to corresponding obligations today, especially where services are offered in the area of cloud services and IT infrastructure whose failure affects a correspondingly large number of users.

In this context, it cannot be ruled out that automobile manufacturers will also be obliged to comply with corresponding requirements in the future.

With regard to the automotive industry, the requirements of the Chinese Draft Provisions are likely to exceed the currently applicable requirements within the EU, at least as things stand today, although it does not seem unlikely that the standards will be harmonized in the near future.

The debates that have been going on for many years under European data protection law about the permissibility of transferring personal data to bodies outside the European Union are likely to become increasingly important for automotive companies in China in the future with the new Chinese Draft Provisions. In particular, the requirement for a state-organized data export security assessment is likely to have a major impact on the future processes of internationally operating manufacturers and service providers who rely on the transmission of vehicle data across national borders to provide their services. While it remains to be seen how the regulations will ultimately be implemented in Chinese law and how the requirements will be specified by Chinese authorities, it is already clear that internationally operating manufacturers and service providers will have a lot of work to do in this area.

Chinese draft car data law vs. GDPR – Major Take Aways

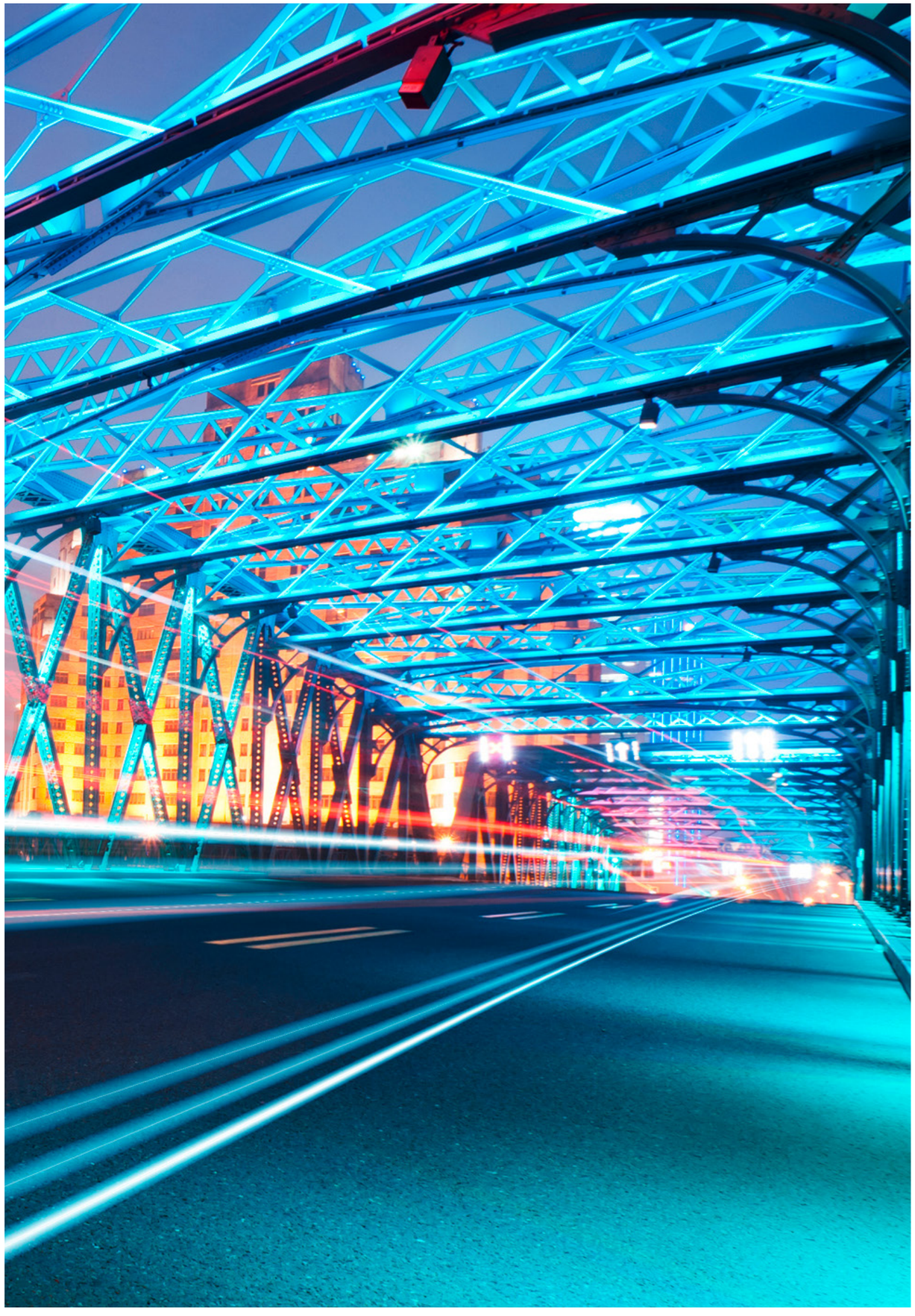
While the GDPR may have been a good guideline for car manufacturers and automotive companies in recent years for the design of concepts for handling vehicle data, it is becoming apparent that other countries such as China and the US are following suit and may even overtake European supervisory authorities in data protection in the future. As in many other industries, the question for companies in the future will be which privacy regime will form the “gold standard”.

Orientation to the requirements of the GDPR and the most recently issued Guidelines certainly still offers companies a variety of practical advantages. For example, European supervisory authorities have already drawn a comparatively detailed picture of the implementation of data protection requirements in the automotive sector and have been actively involved in the development and implementation of corresponding technologies and concepts in the past.

However, depending on the importance of the respective market for manufacturers and providers, this focus may shift in the future and legal requirements from other parts of the world may become significantly more important in the development of new technologies.

The Draft Provisions for China take a rather strict approach and regulate data topics in the automotive industry in a quite comprehensive and far reaching sense. Certain provisions like reporting obligations and data onshore storage requirement will create challenges for the most often internationally active OEMs and suppliers who certainly would highly benefit from aggregation of their global data and equal requirements on a global scale. Tesla’s recent announcement to set up its local data center in China is surely one response of international OEMs to the intensified data compliance requirements in China but most probably not the final and overall answer how to stay compliant. There are many other aspects to watch out for (e.g. pedestrian privacy protection, etc.). Given the size of the Chinese auto market, all participants in the automotive industry, whether production or service should start to plan actions to accommodate the new compliance challenges that may be brought by these Draft Provisions and further rules most likely are to come in the near future.

Manufacturers who have so far based their concepts exclusively on the GDPR have created a good basis for being compliant under Chinese law in the future. As we have seen, in the future it will be necessary for all manufacturers and suppliers in the Chinese market to take a close look at the Chinese regulations to be applied to the handling of vehicle data, as the respective requirements in individual areas go beyond the already strict requirements of the GDPR. Companies in the automotive industry operating in China and the European Union will want to keep a close eye on the legislative process in China (and the EU) in order to be able to react quickly to corresponding requirements - a challenging but certainly equally exciting task!



1000+ lawyers
300+ partners
28 offices
16 jurisdictions

Austria	Klagenfurt | Vienna
Belgium	Brussels
China	Beijing | Hong Kong | Shanghai
Czech Republic	Brno | Prague
France	Paris
Germany	Berlin | Düsseldorf | Frankfurt | Hamburg | Munich
Hungary	Budapest
Netherlands	Amsterdam | Eindhoven
Poland	Warsaw
Slovakia	Bratislava
South Korea	Seoul*
UAE	Dubai
Ukraine	Kyiv
United Kingdom	Cambridge | Liverpool | London | London TechFocus
USA	New York | Silicon Valley

* In association with DR & AJU LLC

TaylorWessing