TaylorWessing

Car Data Protection in the "Extended Vehicle"

Year after year, more and more vehicles on the market are equipped with Connected Car technologies to exchange information wirelessly with mobile apps, the vehicle manufacturer, service providers, other users, infrastructure operators and last but not least other vehicles. It is estimated that 70% of the vehicle population will be connected by 2025. The technologies used enable OEMs in particular to offer new service fields such as a digital "vehicle health monitor" and remote maintenance services: a predictive system that detects malfunctions and sends recommendations and reminders for a visit to the workshop before a component breaks down.

The basis for these business models is a valuable commodity: data. Mobility data is the fuel for every (future) service in the automotive and mobility sector and access to this data enables market participants to develop, offer and provide appropriate services.

This is where a conflict arises between the interests of the players involved: On the one hand, independent market participants ask for sustainable concepts for fair competition, while manufacturers seek a sufficient protection of the investments made as well as existing IP rights and know-how. However, in that equation it remains often overlooked that also data protection and security play a major role, because not everything that is "possible" with vehicle data is also permitted.

In recent years, there has been particularly intensive discussion of the concepts that are intended to give market participants access to data from the connected vehicle, better known as the "extended vehicle" concept.

What is "Extended Vehicle"?

The "extended vehicle" discussion is primarily concerned with the question of whether and to what extent vehicle manufacturers must make available to independent service providers and other market participants (outside the OEMs' own network) the data arising in connection with the operation of vehicles; e.g. to enable other market participants to develop and offer comparable products and services.

Why do manufacturers have to provide data?

Manufacturers are obliged to make certain vehicle data available to other market participants to a certain extent, which in principle follows both from general provisions of competition law (cf. inter alia Art. 102 TFEU and Sections 18 to 20 of the Act against Restraints of Competition [GWB]) and from EU legislation specifically enacted for this purpose. Article 6 of Regulation (EC) No 715/2007 contains specific legal provisions requiring manufacturers to give independent operators access to vehicle repair and maintenance information. Art. 61 et seq. of Regulation (EU) 2018/858, which applies from 1 September 2020, clarifies these obligations.

Nowadays, vehicle data is mainly collected from the vehicle via the so-called Onboard-Diagnosis Interface (OBD), e.g. during a visit to the workshop. As an interface for vehicle diagnostics in the workshop, it is, however, not suitable for access to vehicle data by "new" market participants. In the future, data will increasingly be transmitted from the vehicle to external locations via over-the-air technologies (OtA). They thus offer better technical possibilities for implementing data transmission to the manufacturer – and where necessary to the "aftermarket".

What data must be made available?

Regulation 2018/858, which will apply from 1 September 2020, already contains specific requirements as to which data should be made available and how. For example, Article 61(1) states that *"manufacturers shall provide to independent operators unrestricted, standardised and non-discriminatory access to vehicle OBD information, diagnostic and other equipment, tools including the complete references, and available downloads, of the applicable software and vehicle repair and maintenance information. Information shall be presented in an easily accessible manner in the form of machine-readable and electronically processable datasets. Independent operators shall have access to the remote diagnosis services used by manufacturers and authorised dealers and repairers."*
Thus, Regulation 2018/858 will certainly bring more clarity compared to the previously existing provisions, but many details will remain unclear and controversial. In practice, for example, the question will continue to arise as to what information must now be passed on in what way, in what form and to which third parties. A comprehensive detailed analysis of the planned concepts will therefore be essential for every OEM.

What must be observed with regard to data protection?

However, the discussion on third-party access to vehicle data raises not only competition law issues, but also a number of data protection questions. While competition law deals with the scope of the obligation to provide vehicle data, data protection law to a certain extent takes the opposite perspective: To what extent is the mandatory provision of vehicle data, which regularly includes personal data (e.g. FIN), permissible under data protection law?
The first, albeit rather unproductive, indications for resolving the tension between competition law and data protection requirements are provided by Regulation (EU) No 2018/858, where recital 62 clarifies that data transfers under this Regulation may only be made in compliance with applicable data protection law, in particular the provisions of the GDPR.
Consequently, such data transmission operations should not be justified solely on the basis of the requirements of Regulation (EU) No 2018/858. Rather, they require a comprehensive examination and weighing up against the general principles and conditions of data protection law.

On what legal basis can such a transfer be based?

This depends largely on the specific processing situation. Various scenarios are conceivable here. At first glance, Regulation (EU) No. 2018/858 aims to enable third parties to provide corresponding services in the vehicle ecosystem. Typically, the customer concerned would be likely to request corresponding services specifically from the external service provider or another third party, who would then need access to corresponding data from the customer's vehicle and receive it via a corresponding "extended vehicle" platform of a manufacturer.
If a user expressly requests a corresponding data transfer from the manufacturer, the associated data processing is likely to be carried out regularly in fulfilment of the customer's request, i.e. on the basis of Art. 6 (1) (b) GDPR), but also, depending on the scope of the duties requiring action, possibly based on a legitimate interest of the parties involved (Art. 6 (1) (f) GDPR).
Against the background of the manufacturer's obligations under Regulation (EU) No 2018/858, the transfer of such data to third parties could also be based on the legal basis of Art. 6 (1) (c) GDPR (legal obligation).
The consent of the person concerned in accordance with Art. 6 (1) (a) GDPR also appears possible, but from a pragmatic point of view it is likely to be only the second choice alongside the alternatives mentioned.
However, it remains clear that the transfer of data from a user's vehicle "on his behalf" requires appropriate verification to ensure that the data reaches the "right" place. To this end, manufacturers will (have to) develop suitable concepts, taking into account the specifications on technical and organisational measures in accordance with Art. 32, 25 GDPR, which will enable the transfer of corresponding data to third parties in conformity with the law but also most conveniently from the user's point of view.

What transfer of which data is now required?

Each of the above-mentioned legal bases raises its own questions, but all of them require the examination of the following unresolved issues:

- To what extent do the EU regulations constitute "legal obligations" to process data within the meaning of Article 6(1)(c) GDPR?
- To what extent must an OEM pass on personal data of a vehicle user in order to fulfil its (contractual) obligations towards the respective data subject or its statutory obligations under Regulation (EU) No 2018/858? What is actually "required" in this context, what is not?
- Is "vehicle repair and maintenance information" within the meaning of the Regulation exclusively technical data (which may be assigned to a specific vehicle via the VIN) or can it also include other personal data which may reveal information about the (driving) behaviour of a person (e.g. type of use of a vehicle-related service)?
- Under what circumstances and with regard to which data can the interests of the manufacturer or third par-

ties outweigh the interests of the user?

After a first analysis of the wording of the relevant standards of Regulation (EU) No 2018/858, there is a strong case for exercising restraint in the disclosure of personal data of the vehicle user in any case, if they are not necessary for the specific service requested by the user from a third party.

As to what is "required" under the Regulation (and may thus form a basis for a necessity test under GDPR) existing standards for extended vehicle concepts such as ISO20077, 20078 and 20080 may help to interpret the relevant provisions. The disclosure of "excessive" data, in particular data which allows conclusions to be drawn about (possibly even illegal) user behaviour or other sensitive data, should always be checked thoroughly and, in case of doubt, handled with restraint. Data minimization and privacy-by-default play a central role here in order to develop a viable data protection concept for extended vehicles.

Is the person concerned aware of all relevant data processing?

Last but not least, when implementing an extended vehicle solution, the requirements for providing sufficient information to data subjects in accordance with Article 12 et seq. GDPR must not be forgotten. In particular, those affected must be informed of these requirements,

- which processing steps exactly take place and where the data comes from
- which data exactly are passed on to third parties, and
- to whom the data are disclosed and for what purpose (e.g. only to third parties expressly designated by the data subject).

Extended Vehicle only one of many exciting data protection topics for automotives in 2020

The implementation of extended vehicle concepts will keep manufacturers busy in 2020.

However, the draft of the European Data Protection Board's Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications published in February 2020 is currently providing plenty of food for thought in the industry and has one or two other exciting data protection topics for automotives 2020 in store.

Your Contact

Thomas Kahl
Partner, Frankfurt
+49 69 97130 241
t.kahl@taylorwessing.com

About Taylor Wessing

Leading international full service law firm.

Comprehensive and practical advice on all issues of national and international business law.

Profound **industry know-how** through longstanding relations to leading industrial companies.

Presence in Europe, the USA, the Middle East and Asia, including our cooperation in South Korea.

Strong presence in Asia through our leading China practice.

Expert teams focused on other key economic regions such as Russia, Brazil and India.

In countries where we do not have an office, we work with selected and well-proven partner law firms.