TaylorWessing

Car Data Protection Management in the Connected Vehicle Landscape

Car Data (Protection) Management – A Challenge for Automotives

Connected vehicles generate tremendous amounts of data, which are stored and processed partly inside the vehicle (IN-car) and outside the vehicle (e.g. in the manufacturer's vehicle backend). Data collected from the vehicle is used to provide data-based services in the Connected Car ecosystem but also for additional purposes such as product monitoring, product development, management of warranty and goodwill claims or ensuring the IT security of the vehicle.
Which of the data is recorded in the vehicle and/or transmitted to locations outside the vehicle is primarily decided by the OEM's competent R&D and/or specialist department, which develop and implement the corresponding services.

A Challenge for Legal Departments and Data Protection Organisations

As legal departments and data protection organizations may not always be involved early on in the development process but rather at a later (something the latest stage) this imposes great challenges as the actual permissibility of the actual configurations under data protection law is often only discussed shortly before a certain implementation or technology hits the market.
It is also not uncommon for it to be discovered only afterwards, i.e. after a product has been sold and is then already on the market, that configurations in the vehicle (e.g. which data is collected and stored in the vehicle under what exact circumstances) have not been carried out in a manner that conforms to data protection regulations.

Car Data Protection and the GDPR

According to the principles of the GDPR, manufacturers may under certain circumstances be held responsible for data protection shortcommings even if they were committed by employees at subordinate decision-making levels (principle of so-called „association liability"). In addition, in such cases it is often assumed that the OEM's company management is at fault for the lack of control and implementation of sufficient control systems in the organisation.

According to the principle of accountability (cf. Art. 5 (2) GDPR), manufacturers are obliged to establish appropriate internal control mechanisms in the sense of a data protection management system (DPMS) and to maintain them with sufficient resources. In addition, and even if the GDPR regulations do not make any clear statements in this regard, it has long been recognised, following the agreement of the automobile associations with the German supervisory authorities, that automobile manufacturers must in any case comply with the principles of privacy-by-design and privacy-by-default (cf. Art. 25 GDPR) in the development and configuration process of their vehicles already.

GDPR Risks … and what can become of them!

Against this background, it is advisable for car manufacturers (and their suppliers, where feasible for their products or services) to set up a car data protection management system or corresponding control mechanisms to ensure that data collected in the vehicle can be processed locally (i.e. in the vehicle) and externally (e.g. in the vehicle backend) in a manner that conforms to data protection requirements.
Non-compliant processing of vehicle data may - in addition to sanctions by supervisory authorities - trigger demands by data subjects or associations and consumer protection groups which could be brought against an OEM even by way of an injunctive relief and removal request. In individual cases, it could lead to manufacturers being obliged to technically reverse a certain configuration of processes inside and outside the vehicle that is in breach of data protection law.
When lucky, corresponding adjustments can (still) be realized by remote updates of the software in the vehicle. In other cases, however, this may not be possible without further ado, so that in critical cases (and insofar as all other circumstances are considered to be reasonable), the rectification of corresponding faults could also be obligatory within the framework of customer service measures, which may also include the return of vehicles to the workshop, if this is in fact necessary to rectify corresponding deficiencies – a costly procedure which us usually associated with negative public coverage.

Given the sensitivity of the data often processed in this context and the large number of users usually affected by such errors, the risk of fines in the event of a dispute with a supervisory authority should not be underestimated.

Mitigating risks through a Car Data Protection Management System

In order to avoid these harsh consequences, a control mechanism or process for managing the handling of data in and from the vehicle must be developed.
The aim of such a mechanism should be to ensure that it is known and documented (i) for what purposes a data set in the vehicle was originally created or for what purpose exactly it is to be used, (ii) which parts of the organisation are responsible for or involved in its creation and/or later processing, and (iii) that an adequate data protection review is carried out before the going live of a product or a service.
Such a process may include, but is not limited to, the following elements:

- Creating a guideline for vehicle developers according to the principles of privacy-by-design and privacy-by-default (subdivided, if necessary, according to general principles, topic-specific requirements (e.g. special topics for autonomous driving) and short checklists for the business units for their day-to-day business)
- Documentation of the relevant data sets in the vehicle, to be recorded and described by the respective "data (or process) owners" according to purpose / area of application and other relevant aspects
- Defining a process which helps with the maintenance of such a documentation including a process for applying it to new development initiatives and new products or services
- Create a process for checking and documenting car data and processing purposes in accordance with GDPR (e.g. by implementing a risk assessment system based on points/scores, escalation procedures and decision making processes)

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.

© Taylor Wessing 2020

This publication is not intended to constitute legal advice. Taylor Wessing entities operate under one brand but are legally distinct, either being or affiliated to a member of Taylor Wessing Verein. Taylor Wessing Verein does not itself provide services. Further information can be found on our regulatory page at taylorwessing.com/en/legal/regulatory-information.