TaylorWessing

Connected Cars, Cyber Security & Data Protection Challenges

The latest draft of the UNECE WP.29 regulations on vehicle cyber security stipulates that in future, automobile manufacturers must implement a Vehicle Cyber-Security Management System (CSMS).

This step seems to be a logical one: cyber attacks on connected vehicles can pose a considerable threat to the safety of vehicle occupants and thus to road safety, which is why the pressure on vehicle manufacturers to establish appropriate security architectures in a timely manner is increasing.

Data Protection – Why would that be a topic here?

Data, including (personal) vehicle data, are indispensable for monitoring the respective ecosystems due to product observation and monitoring legislation. In order to obtain the broadest possible database for cyber security monitoring purposes, the processing of vehicle data is inevitable. The processing procedures usually gain relevance in terms of data protection law by linking a data record with the respective vehicle identification number (VIN) or other identifiers. However, the use of (personal) vehicle data underlies restrictions under the EU General Data Protection Regulation (GDPR) and other data protection driven regulations. How the tension between data protection on the one hand and product liability and monitoring requirements on the other can be reasonably resolved is not answered by the currently available legal requirements.

As the new regulations are aimed at becoming binding law by 2022 the compliant design of such an CSMS will become one of the major challenges for automotive manufacturers in the near future.

Cybersecurity in the connected vehicle – How does that work?

Cyber attacks on the ecosystem of the connected vehicle can be carried out using a wide range of attack angles. Particularly relevant are interfaces through which hackers can gain access to the respective infrastructures (including operating interfaces in the vehicle, the OBD-2 interface or wireless communication interfaces).

In order to detect and manage cyber attacks on the connected vehicle, so-called Intrusion Detection (IDS) or Security Information and Event Management (SIEM) systems are used. The respective systems and processes will be managed by a Security Operations Center (SOC). The core idea of a SIEM is to monitor activities inside and outside the connected vehicle in order to detect – rule-based, but in future also with the help of machine learning – activities and anomalies that indicate a cyber attack with potentially damaging consequences.

What's the current legal framework for cybersecurity in the connected vehicle?

According to the specifications of the UNECE draft on cybersecurity, automobile manufacturers will have to implement a certified CSMS in the future and maintain it throughout the entire life cycle of the vehicle. The specifications pose particular challenges for producers, especially because cyber risks will often be only partially predictable at the time of the conception of the vehicle and its security mechanisms. The requirements are

specified by the SAE/ISO industry standard 21434 on cybersecurity published in parallel in a draft version.

In addition, there are various industry-independent IT security requirements that might also be relevant to cybersecurity in the vehicle, such as the Cybersecurity Regulation (EU) 2019/881 and the BSI Act (BSIG). Specifications on data security can also be found in the general provisions of the GDPR, including Art. 32, 25, etc. The respective specifications are concretized by individual statements by data protection supervisory authorities, including the statement by the French data protection supervisory authority CNIL and the European Data Protection Board (EDPB, not adopted draft version of the guidelines for data protection in the connected vehicles landscape), which deal with data protection in the environment of connected vehicles.

Cybersecurity – What's the background from a product liability and monitoring law perspective?

Both the product monitoring obligation and the obligation for effective risk control are aspects of the vehicle producer's safety obligations under producer liability law. The producer's obligations are therefore such that he must use all measures available according to the current state of the art to ensure the safety of his product – as far as reasonable in relation to the risk posed – and observe his product after it has been placed on the market so that he can take risk control measures if any (imminent) dangers are detected. If the producer does not sufficiently comply with his obligation to observe the product and accordingly cannot react in time to avert or effectively control the danger emanating from the product for the customer, under German law he would be liable for the damage caused by this violation of the obligation to react accordingly.

With connected vehicles, the new forms of remote data access may technically enable the producer to monitor the condition of a device placed on the market as well as any malfunctions / faults of the respective products. However, whether this theoretical possibility of obtaining information can be used to derive a corresponding obligation on the part of the producer is currently the subject of controversial debate.

In any case, the implementation of such an "obligation to inspect" will nevertheless have to comply with the limits of data protection law, which is certainly the biggest legal hurdle in this context. As a result, especially in the case of connected vehicles, due to the safety relevance and the potential danger to life and limb, it cannot be ruled out that a producer will be liable in tort if he refrains from a possible and reasonable use of the „new" possibilities to technically monitor the vehicle, e.g. through a SIEM system.

The specifications of the UNECE draft regulation on vehicle cybersecurity, which expressly makes appropriate monitoring of the vehicle or its functions a prerequisite for approval, also point in this direction.

Another question that is currently still controversially discussed is whether a producer, if it becomes aware in particular of security gaps in certain networked products, is obliged as part of its safety obligations to provide appropriate software updates to close the security gaps (free of charge) or may even be obliged to immobilise a vehicle by remote control. Another thrilling topic which shall, however, not be further elaborated on at this point.

SIEM & Data Protection – Does that work?

At first sight, the consultation version of the EDPB's Connected Vehicles Guidelines published in February 2020 gives rise to the question of whether data processing for the purposes of a SIEM might be subject to more general data protection law "showstoppers".

A first hurdle could result from the very strict application of Art. 5 para.3 of the ePrivacy Directive to vehicle data, as it seems favoured by the EDPB. According to this, the processing of vehicle data should in many cases be based on consent. This seems questionable for several reasons – one of them being that it is already unclear whether the EDPB had data processing for cybersecurity purposes in mind when making its statements.

The significance of Art. 10 GDPR (as highlighted by the EDPB in namely that guideline) for SIEM processes also seems questionable, if and because with SIEM circumstances such as the hack of a vehicle could be uncovered which could be deemed a conduct that may be relevant under criminal law.

Although EDPB has not yet issued the final version of its guidelines, it seems hard to believe that the aforesaid aspects could become a general showstopper for SIEM data processing activities. In any case, companies will have to wait and see how the EDPB will position itself.

SIEM & Data Protection – How can it be justified?

In any case, the processing of personal vehicle data for the purposes of the SIEM requires permission under data protection law (cf. Art. 5 para. 1 (a) GDPR).

Data subject consent (Article 6 para. 1 (a) GDPR) or a contract with a customer (Article 6 para. 1 (b) GDPR) will usually not be a suitable approach for manufacturers due to various practical downsides.

As the operation of a SIEM is supposed to help car manufacturers to comply with their product monitoring obligations the first thing that comes to mind would be to argue that any related processing is to be based on that particular legal obligation (cf. Art. 5 para. 1 (c) GDPR). However, the conditions for this are controversially discussed, especially where relevant obligations result not from written law but mere judicial law.

Such an obligation could, however, be seen in the UNECE (WP.29) regulations. For data processing operations described in the standards, classification as a "legal obligation" within the meaning of Art. 6 para. 1 (c) thus seems possible, or at least at first glance, as there are – again – many further hurdles to take, including the unclear relation between for example the GDPR and the UNECE (WP.29) regulations. For processing operations in a SIEM which cannot be derived directly from the UNECE regulations or which are (only) carried out in fulfilment of the requirements of unwritten (legal) obligations, the path via Art. 6 para. 1 (c) is likely to be (even) more difficult.

In view of these circumstances, Article 6 para. 1 (f) is of major importance for SIEM. When following this path, the balancing of interests must take into account various aspects, including the nature and weight of the interest in the purpose of the data processing (e.g. overlap with public interests), the consequences where such a procedure might not be implemented, the objective expectations of the data subject, the sensitivity of the data processed or the manner and means by wich the data are processed.

The balancing of interests will rather be positive where high-level legal interests (life and limb) are to be protected. In any case, the legal obligations of the manufacturer (including those resulting from the UNECE (WP.29) regulations) must be taken into account as a decisive factor in the balancing of interests. Where such obligations exist, they will often be an indication of a positive balance of interests in favor of the manufacturer – if the processing occurs within the "guard rails" of data protection law.

SIEM & Data Protection – What are the major guard rails and design options to consider?

1 Provide for early on data minimization and „privacy by design"

When designing the respective processes, the principles of necessity and data minimisation (cf. Art. 5 para. 1 (c)) must be observed first and foremost. A distinction must be made between the processes in the vehicle, the collection from the vehicle and the processing of the collected data in the SOC for the purpose of attack detection and management. According to the principle of privacy by design (cf. Art. 25), only the data that is actually required for the subsequent processes should be collected in the vehicle.

The intervals at which corresponding data are collected from the vehicle are likely to be an important data protection "set screw". In the case of collection during a workshop visit, processing for cybersecurity purposes should be possible under less strict conditions than in the case of over-the-air (OtA) vehicle data collection at regular intervals or even by means of real-time monitoring. The permissibility of the latter should depend, inter alia, on the risks and its likelihood of occurrence, thus facilitating the close monitoring of cybersecurity where the protection of life and limb is at stake or where such risks are particularly imminent.

Within the framework of the evaluation processes in the SOC, it will be essential to ensure that data evaluation is carried out strictly according to the need-to-know principle. Data access to different data categories must be secured by appropriate access authorisations. As far as possible, evaluations should be based on anonymised or pseudonymised data. Access to data that individualise a specific vehicle should only be possible under strict conditions.

Insofar as data were originally collected for other purposes and are to be merged with the data in a SOC, their use would have to be measured against the requirements of Art. 6 para. 4 or the corresponding standards of the Federal Data Protection Act (BDSG) (change of purpose).

2 Store and delete data adequately

The permissible duration of data storage in a SOC must be determined on the basis of a necessity analysis. Depending on the processing purpose and the objective of the evaluations, short storage cycles may be necessary

in individual cases. On the other hand, longer storage periods, e.g. several weeks, months, etc., may be permissible where only a long-term view would permit an efficient analysis. The sensitivity of the stored data will also play a role in the analysis. In any case, special protective measures are to be taken as far as possible (including encrypted storage, pseudonymisation or "blocking" of data).

3 Assess special processing scenarios with dilligence and care

Moreover, the admissibility of processing in a SOC is likely to depend very much on the sensitivity of the categories of data concerned. The processing of position data in the vehicle environment is often evaluated critically. However, while the processing of position data for SIEM purposes should likely be possible, the processing details will certainly be subject to – sometimes even severe – restrictions. Corresponding data should be anonymised or pseudonymised as early as possible (e.g. by targeted "blurring" of location data). If location data subject to applicable telecommunications regulations is processed, further special requirements might be of relevance. Further restrictions may also result from the group of data subjects concerned. For example, when processing employee data for SIEM purposes, more detailed requirements acc. to national law or restrictions under individual and/or collective labour law may also have to be observed.

4 Implement adequate organisational measures and regard data subject rights

In addition further steps will be necessary to make a SIEM process compliant with data protection requirements. Data subjects must of course be adequately informed about the processing in question. According to the principle of accountability, comprehensive documentation of the processes, including access and authorisation concepts, documentation of system accesses, responsibilities and decision-making processes, as well as an adequate data storage and deletion concept will become mandatory. Due to the comprehensive data processing associated with the corresponding processes, the implementation of a privacy impact assessment is likely to be unavoidable. The extent to which consultation with the competent supervisory authority will also be necessary remains to be examined in each individual case.

What's to take awyay from it for car manufacturers?

Car manufacturers are facing great challenges in view of the growing cyber dangers, the high time pressure in implementing the new regulations and the risks of sanctions under data protection law. From a data protection point of view, it is unfortunate that the existing regulations on cyber security in the vehicle do not yet provide a clear framework for the admissibility of such processes under data protection law. Until then, it should be possible to develop practical solutions for SIEM processes on the basis of the existing regulations, which can be brought in line with data protection regulations.

An essential success factor for car manufacturers will be to integrate the data protection perspective into project planning at an early stage and to merge it with the product liability perspective – so that data protection does not become a "showstopper" but a "selling point" for corresponding solutions.

Your Contacts

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

Dr. Philipp Behrendt
Partner, Hamburg
+49 40 36803-141
p.behrendt@taylorwessing.com