The voice of European vehicle dealers and repairers

cecra.eu

Brussels, 10/04/2020

CECRA Response to EDPB Guidelines on processing personal data in the context of connected vehicles and mobility related applications

ABOUT CECRA

CECRA is the European umbrella association of the motor trade and repair sector representing the interests of both, franchised vehicle and truck dealers and independent repairers. In Europe there is a total of 46,720 vehicle and truck dealers and 290,000 repairers. Those – predominantly small and medium-sized – companies employ approximately 2.9 million people being responsible for the sale of almost 16 million new vehicles a year as well as the repair and maintenance of the 228 million existing passenger vehicles and 38.5 million commercial vehicles. Thus it is ensured that vehicle users in Europe can rely on a network of qualified experts for the purchase and maintenance of their vehicles.

European Council for Motor Trades and Repairs

Boulevard de la Woluwe 46, box 9 · 1200 Brussels – Belgium · t. +32 (0) 2 771 96 56 · f. +32 (0) 2 772 65 67 · mail@cecra.eu

CECRA supports the EDPB's goal of clarifying the implications of the GDPR and the e-Privacy Directive on the use of personal data in connected vehicles and mobility applications.

European motorists are willing to embrace car connectivity[1], provided that they know which data their vehicle shares and are given a real choice with whom they wish to share data.

Currently, only vehicle manufacturers have access to this data for specific vehicle models.
Vehicle manufacturers (OEM) currently propose the Extended Vehicle concept, which forecast the access to a limited amount of data via servers solely under their control. In this technical architecture, all vehicle data are transiting via manufacturer servers and only OEMs have privileged access to the customer's dashboard and personal information, making the manufacturers the only data controller.

CECRA, among a broad coalition of organisation representing the automotive aftermarket industry, undersigned the Manifesto for fair digitalisation opportunities[2], in which we call for a Shared data server solution combined with an open in-vehicle platform.

In this scheme, the in-vehicle architecture should be adapted to include an on-board application platform (OBAP) or open telematic platform (OTP). This platform could support different functionalities directly from the dashboard or the telematic control unit (TCU) HMI. Data transfer would be split to provide differentiated access to the vehicle manufacturer and independent service providers (ISP). Access to vehicle data will always be subject to obtaining the informed driver consent. Vehicle data would be transferred anonymously and securely to the vehicle manufacturer's server or to the ISP's servers depending on the one authorised/selected by the driver.

Therefore, we welcome the EDPB guidelines as they take into account the suppliers of the automotive aftermarket in several points.

We salute the fact that a more open interaction with the driver is advised and that vehicle data are processed under the General Data Protection Regulation.

In addition, we value that the EDPB recommends developing a secure in-car application platform, physically divided from safety relevant car functions so that the access to car data does not depend on unnecessary external cloud capabilities.

Nevertheless, we would like to address that the EDPB guidelines, while granting a solid data protection framework, still doesn't successfully allows for competition in the aftermarket in the connectivity context for all service providers.

1 FIA Region I, "What Europeans think about connected cars", Brussels, January 2016
2 FIGIEFA, Manifesto for fair digitalisation opportunities, Brussels, October 2019

In that sense, EDPB guidelines, still lack of clarity and consistency, especially on the following points :

Art.25 GDPR requires that data controllers must apply the obligations of Data protection by design and by default.
Nevertheless, paragraph 68 draw attention to the lack of specific guidance on how OEMs can comply with data protection by design and default.
This situation can lead to a voluntary restriction, by OEMs, of the possibilities of installation of an on-board application. Where, paradoxically, paragraph 70 emphasis on internally processed data that presents fewer cybersecurity risks and involves little latency.

Also, Art.5(3) ePrivacy directive raises the question of the consent of the consumer in order to gain access to information that is already stored in the vehicle and collected through a publicly available electronic communication service.
However in the Extended Vehicle concept all electronic communication service are the propriety of OEMs.
Finally, regarding paragraph 105, attention should be made on the risk of a holdup on the part of the OEMs at the signing of the purchase of a vehicle, leaving no room for 3rd parties.