

Deliberation 2021-036 of March 30, 2021 Commission Nationale de l'Informatique et des Libertés Nature of the deliberation: Opinion Legal status: In force Date of publication on Légifrance: Saturday December 25, 2021 Deliberation n° 2021-036 of March 30, 2021 providing an opinion on a draft ordinance resulting from article 32 of the mobility orientation law relating to access to vehicle data (request for opinion no. 21003506) The National Commission for Computing and Liberties, Seizure by the Minister Delegate in charge of transport for a request for an opinion concerning a draft ordinance resulting from article 32 of the mobility orientation law relating to access to vehicle data; Having regard to regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR); Law No. 78-17 of January 6, 1978 modified relating to data processing, files and freedoms; Considering the law n° 2019-1428 of December 24, 2019 of orientation of mobility, in particular its article 32 (LOM); After having heard Mrs. Marie-Hélène BOIDIN-DUBRULE, commissioner, in his report, and Mr. Benjamin TOUZANNE, government commissioner, in his observations. Issues the following opinion: -1428 of 24 December 2019 mobility orientation (LOM). This project plans to make relevant data from systems integrated into motorized land vehicles accessible to: road infrastructure managers, law enforcement and fire and rescue services for the purpose of detecting incidents and accidents and the conditions dangerous traffic; to the manufacturer, as part of the reinforcement of the safety of the driving delegation systems. In the event of a road accident, the data from the event recording devices (EDR) and the state data delegation of driving (DSSAD) will be made accessible: to officers and agents of the judicial police for the purposes of the study and analysis of accidents for the determination of responsibilities, and to the organizations responsible for the technical investigation and the safety investigation, for the sole purpose of studying and analyzing accidents; to insurers and, where applicable, to the guarantee fund provided for in this area, with regard to state of delegation of driving, for the purpose of determining the necessary compensation. its equipment; to road infrastructure managers and mobility organizing authorities for the purpose of knowing road traffic. Finally, it plans to allow the telematic correction of vehicle safety defects. the Commission had been asked for an opinion in 2018 did not contain the provisions of Article 32, from which the draft ordinance, the subject of this opinion, results. It was therefore unable to comment on the principles provided for in this article. The question of the legitimacy of access to and transmission of data The draft ordinance provides for the access and transmission of data from vehicles connected to the benefit of many actors, whether public bodies (police forces and fire and rescue services, etc.) or private bodies (road infrastructure managers, etc.). As a preliminary point,

the Commission points out that the organization of access to data from connected vehicles for the benefit of these players is provided for, on the one hand, by the LOM and, on the other hand, by European regulations, like EDRs to which access by national authorities is permitted by Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on the general safety of vehicles on the basis, in particular, of national law. many purposes provided for by the draft ordinance (detection of accidents and dangerous traffic conditions, knowledge of the state of the infrastructure and its equipment, study and analysis of accidents, etc.) should in particular make it possible to reinforce safety of road transport and the quality of interventions in the event of an accident and therefore pursue an important public interest. However, the Commission wonders about the compatibility of access, by judicial police officers and agents, to data from event recorders with a view to determining responsibility in the event of a road accident (draft article L.1514-4 of the transport code), with the provisions of the aforementioned European regulation 2019/2144. Firstly, the Commission notes that the provisions of Article 6.4 of the European regulation, which come into force on 6 July 2022, provide that EDR data may be communicated to national authorities, on the basis of national law, for the sole accident study and analysis requirements. The CNIL wonders about the possibility of extending the use of data collected by EDRs beyond these purposes, by including the determination of the responsibilities of the people involved in the accident, within the framework of an investigation or secondly, it points out that the regulation mentions that EDRs should operate according to a system which, on the one hand, does not allow the identification of the vehicle or its holder (article 6.4 uses the term of anonymized data) and, on the other hand, allows an overwriting of stored data. Furthermore, pursuant to Article 6.5 of the Regulation, such a device must not be capable of recording and storing the last four digits of the vehicle designation part of the vehicle identification number, nor any other information which could allow the individual identification of the vehicle concerned, its owner or its holder. Therefore, the logic of separation between data relating to accidents and personal data of the driver does not seem to be able to be respected in the context of access to data collected and stored in an identifying manner for the six years provided for by the text, for the purpose of establishing in particular the level of responsibility of the driver. The draft ordinance provides, in draft article L. 1514-5 of the transport code, equivalent provisions (purposes, accessors, retention period, etc.) to those of the EDRs, for the DSSADs. In this regard, the Commission takes note of the Ministry's clarifications that DSSADs are currently the subject of regulatory work at the international level. The Commission invites the latter to take account of the conclusions that will be taken by the competent international bodies, particularly with regard to the data made accessible and the quality of the users or recipients. More

generally, the Commission notes that the draft articles mentioned above impose, by way of ordinance, on private actors offering connected consumer goods, the implementation of systems making it possible to monitor the use of these goods and to verify, during any criminal investigations carried out later, the conditions of use thereof. These measures are based on a logic of traceability of the actions of the driver in his vehicle, without control by the latter over his data, a logic which carries risks for individual freedoms and is likely to amplify the feeling of surveillance of citizens even in their vehicles. Thus, without calling into question the possibility for the police, in a judicial context, to request the communication of any available element contributing to the manifestation of the truth according to the procedural rules provided for in this matter, the Commission recalls that 'Such a possibility does not, in itself, justify the creation of an obligation for manufacturers and constructors to provide for the conservation, within event recorders integrated into their products, of the trace of the conditions of use of these. In addition, the principle of proportionality provided for by the GDPR opposes the general retention, by default, of data affecting the privacy of individuals. The framework for processing operations aimed at accessing or allowing the transmission of information to from vehicles Certain provisions of the draft ordinance specify that data may be transmitted or accessed via communication networks open to the public (draft articles L. 1514-1, L. 1514-2, L. 1514-3 and L. 1514-7 of the transport code). The provisions of Article 82 of the Data Protection Act, which transposes Article 5(3) of Directive 2002/58/EC of July 12, 2002, known as privacy and electronic communications, impose, apart from the applicable exceptions , the collection of the user's consent before any processing operation aimed at accessing or recording information, independently of the qualification of personal data, in the user's terminal equipment. However, Article 1 of Directive 2008/63/EC of June 20, 2008 defines terminal equipment as any equipment which is connected directly or indirectly to the interface of a public telecommunications network to transmit, process or receive information. Consequently, Article 82 is likely to apply to the operations of data transmission or remote access to devices integrated into vehicles by the interface of a public telecommunications network, which would be carried out within the framework of the project prescription. These provisions apply whether the data collected through these operations are of a personal nature or not, since they are intended above all to protect the integrity of the terminal and its confidentiality, insofar as [...] any information stored on this equipment is part of the user's private life, which must be protected under the European Convention for the Protection of Human Rights and Fundamental Freedoms, as recalled in recital 24 of the aforementioned directive of July 12, 2002. Also , in the event that the accesses and transmissions provided for by the draft ordinance would take place remotely via a public telecommunications network, the consent of the users - understood as the

users of the vehicle - should be obtained beforehand to any access or transmission, unless these operations fall within the scope of the exceptions provided for in the aforementioned article 82, namely that they only serve to facilitate or allow re communication by electronic means or if they are strictly necessary for the provision of an online communication service at the express request of the user. The Commission notes, in this respect, that none of the purposes targeted by the draft d ordinance does not seem to fall within the scope of these exceptions. However, some draft articles specify that the consent of the person concerned for the processing of data is not required (draft articles L. 1514-1, L. 1514-2, L. 1514-4, L 1514-5, L. 1514-6, L. 1514-7 and L. 1514-8 of the transport code). The Commission therefore wonders about the possibility of excluding the collection of people's consent with regard to the applicable texts, unless the ministry intends to link the access concerned: either to the areas excluded from the scope of Directive 2002/58/ EC by its Article 1; or to the derogations provided for by Article 15 of Directive 2002/58/EC, in particular in that it provides that Member States may adopt legislative measures aimed at limiting the scope of the rights and obligations provided for in Articles 5 [...] of this Directive where such a limitation constitutes a necessary, appropriate and proportionate measure, within a democratic society, to safeguard [...] public security, or to ensure the prevention, research, the detection and prosecution of criminal offences; or the transposition of the provisions of a European directive or regulation expressly derogating from the provisions of the aforementioned directive. On this point, the Ministry re clarified that the purposes covered by the draft articles L. 1514-1 (detection of accidents and dangerous traffic conditions), L.1514-2 (knowledge of the state of the infrastructure and its equipment) , L. 1514-4 and L. 1514-5 (access to data for the benefit of the organizations responsible for the technical investigation and the safety investigation to the data of the event and status recorders of the delegation of control) of the transport code contribute to road safety: prevention of accidents or improvement of intervention in the event of an accident, knowledge and mapping of the state of assets making it possible to identify anomalies in the state of the infrastructure that could generate accidents, study and analysis of accidents making it possible to learn lessons on transport systems and thus avoid new accidents. The ministry intends to link the concept of road safety to the purpose of public safety explicitly excluded from the scope of a privacy and electronic communications directive . While road safety can be understood as a component of public safety, itself linked to public order, the Commission nevertheless points out that the prevention of breaches of public order and, in particular, breaches of the safety of persons and property, falls under the missions devolved to the public authorities. It therefore invites the Ministry to ensure that the actors accessing data as part of a public security policy fall into this category. With regard to the provisions of draft article L. 1514-7 of

the transport code telematic correction of certain security defects), the Commission notes that if the purpose of the text pursues a legitimate interest and contributes to the proper functioning of the service provided by the vehicle, this is not covered by the exceptions to the principle of consent. On this subject, it notes that the ongoing debates on the revision of Directive 2002/58/EC have led, in the final state of the draft text on the day of this deliberation, to the inclusion of an exception to prior consent specifically applicable to this scenario, together with certain conditions. As these provisions are still under discussion, the Commission can only draw the Ministry's attention to the need to take the greatest aforementioned force. It emphasizes that the interest of these corrections, and the comfort provided by the possibility of remote updating avoiding having to move the vehicle to the workshop, seem likely to win the support of the persons concerned and to facilitate the collection of their consent. Finally, the draft article L. 1514-8 of the transport code provides that when the data collected by the automation system of a land motor vehicle with driving delegation characterizes driving scenarios used for the type approval of vehicles, these are made available to the bodies designated by the Minister responsible for transport to develop these scenarios according to the procedures set by regulation and this, without the prior consent of the users being required. On this point too, the Commission wonders about the relationship between this provision and Article 82. It recalls the need to justify the absence of obtaining consent with regard to Directive 2002/58/EC or other rules of law that would be applicable. Assessment of the project with regard to the provisions of the GDPR, in particular the protection of personal data of the vehicle from the design and by default As a preliminary point, the Commission notes that the order does not mention the exact nature of the data collected, the frequency of the collection or the extent of it. In the absence of visibility from the Ministry on these various elements, the Commission's remarks are of a general nature and do not prejudge a more in-depth analysis that it could carry out in the context of an opinion on a draft decree. of application. The issue of vehicle data protection has been addressed by the European Data Protection Board (EDPB) in its guidelines relating to the processing of personal data in the context of connected vehicles and related applications. to mobility, which testifies to the interest taken by the European data protection authorities in this subject. The Commission notes that the connectivity of these vehicles involves the collection of data sometimes affecting the private movements, driving behavior, etc.) and raises serious questions in terms of the protection of personal data and respect for fundamental rights and freedoms. Consequently, these systems must offer the best possible guarantees to protect the confidentiality of their users' data, allow respect for the freedom of drivers to come and go anonymously and ensure the availability and quality of the information delivered to drivers and automated equipment in

vehicles. The Commission recalls that the personal data produced by the vehicle are protected by the GDPR, and that access to them and the resulting processing cannot have the effect of reducing the level of protection some people. Thus, such access cannot have the effect of creating, for the benefit of vehicle manufacturers and any other actor, a right to systematically collect the data produced by the vehicle or to consider themselves as the owner. Regarding the local processing of personal data, the anonymization of data and the role of manufacturers

The draft articles L. 1514-1, L. 1514-2, L. 1514-3, L. 1514-4 , L. 1514-5 of the Transport Code place manufacturers at the heart of the data access mechanism but do not specify their roles and obligations. respect the privacy of individuals by applying data protection by design and by default obligations, in accordance with Article 25 of the GDPR. Thus, the Commission draws the Ministry's attention to the fact that the integration, from the design of the vehicle, of the techniques described below, can contribute to mitigating the risks for the rights and freedoms of natural persons associated with connected vehicles. On the local processing of personal data The Commission considers that, from the design phase, vehicle equipment should be configured so that only relevant data can be collected and then stored locally, and provision should be made for mechanisms to secure the transmission of this data, by recovering, on a case-by-case basis, only the data strictly necessary to satisfy the purposes referred to in the relevant provisions, depending on the quality of the recipient of the data. Local data processing , i.e. inside the vehicle and without remote access, is to be preferred when the provisions submitted to it indicate nt that the data [...] are made accessible [...] by the manufacturer of the motorized land vehicle or his representative, without providing for an obligation for systematic collection and by default of the data concerned by the manufacturer, nor for an obligation to store these data in remote servers for the purpose of subsequent provision to third parties authorized by law. Such systematic collection by default does not seem to be able to be based on a legal obligation imposed on the manufacturer, with regard to the draft articles submitted to the Commission, which only refer to the fact of making the data produced by the vehicles accessible and not , the implementation of prior processing carried out by manufacturers for the purposes of subsequent provision of data for the benefit of authorized recipients.

On data anonymization techniques The draft articles relating to data allowing the detection of accidents and dangerous traffic conditions, knowledge of the state of the infrastructure and its equipment, as well as those allowing knowledge of the traffic (draft articles L. 1514-1, L. 1514-2, L 1514-3 and L. 1514-8 of the Transport Code) provide that this data is anonymized by a process guaranteeing the irreversible deletion of the link between said data and the serial number or any ident ifying . The Commission recommends, where technically possible, that this anonymisation be carried out inside the vehicle. It recommends that regulatory texts

require manufacturers to integrate anonymization mechanisms when designing integrated systems or any device aimed at producing data within vehicles. In order to ensure effective anonymization, the processes of anonymisation techniques implemented must respect the three criteria defined in the opinion of the group of article 29 n° 05/2014 on the techniques of anonymisation (individualisation, correlation and inference). If these three criteria cannot be met, a study of the risks of re-identification must be carried out in order to demonstrate that the risks associated with the production and provision of the anonymous data set have no impact on the privacy and freedoms of data subjects. In this regard, particular vigilance must be ensured with regard to certain data (for example, time-stamped geolocation data or data produced by camera-type sensors), the anonymization of which could prove to be more complex. and, in the event of failure, a source of risk for the privacy of the persons concerned. The Commission stresses that the mere deletion of the serial number or any other identifier cannot guarantee the anonymity of the data concerned and recalls that in the absence of complete anonymization, the GDPR is fully applicable. On the role of manufacturers The Commission regrets that the draft does not give any indication of the status of the manufacturers with regard to the data processed, namely whether they act as an independent data controller, joint data controller with the recipients, or subcontractor of the latter . Determining their status is a necessary prerequisite for clarifying their obligations, in particular vis-à-vis the persons concerned by the data processed, as well as the purpose of the processing they would like to carry out on the data. With regard to compliance with the principle minimization of data The Commission takes note of the clarifications of the Ministry according to which most of the data will be defined by regulation or come under international regulations in force (for example, for EDRs) or under discussion (for example, for recorders driving delegation status). The Commission will be particularly vigilant about the proportional nature of the various mechanisms envisaged by the text, particularly with regard to data from the DSSADs made accessible to insurers by draft article L. 1514-6 of the transport code. security The Commission emphasizes that while the draft text submitted to it for opinion does not specify the practical methods of data processing or the associated security conditions, the processing concerned will relate to potentially very intrusive data and will ultimately concern a very large number of citizens. Consequently, the Commission will be particularly vigilant about the conditions for implementing this processing: compliance with the security obligation imposed by the GDPR requires that each link in the data processing chain implement the necessary security measures. .In practice, the Commission considers that particular care should be taken in the management of data access authorizations, in the traceability measures for the operations carried out by the authorized persons, in the encryption of the data exchanges carried out between the

vehicles and the infrastructure used, as well as the framework for the operations entrusted to subcontractors and the security objectives that will be set for them. Finally, the Commission also recalls that the processing operations envisaged are, for a very large part of them, subject to the obligation to carry out a data protection impact assessment, which must be regularly updated.

**t retention periods** The draft ordinance provides for particularly long data retention periods for EDR and DSSAD data, without excluding storage outside the vehicle. Indeed, draft articles L. 1514-4 and L. 1514-5 of the Transport Code provide, for the purposes referred to in these provisions, that EDR and DSSAD data will be kept for six years from the date of the accident in question, by the vehicle manufacturer (this period corresponding to the statute of limitations in tort). The Commission stresses that such a retention period poses the risk of leading to the creation of files for the continuous monitoring of driving delegation statuses and data linked to events of all motorized land vehicles subject to French law, placed under the responsibility of manufacturers, files whose supervision raises many questions with regard to the principles of protection of personal data.

complies with the requirements of the aforementioned European regulation 2019/2144 (obligation to anonymize data and data overwriting system). The similar retention period for DSSADs raises questions about the storage methods during this period (local or outside the vehicle) and the actors who will be responsible for it. The draft article L. 1514-6 of the transport code provides, meanwhile, that DSSAD data will be kept for ten years from the date of the accident considered by the vehicle manufacturer for insurers and the insurance guarantee fund. This period corresponds to the limitation period for civil liability actions (of the victim against the insurer of the person responsible) in the case of bodily injury. However, in reality, it is possible that the accident vehicle that generated this data was destroyed and recycled during this period. The question of access to and storage of data over such a period will inevitably arise.

the effectiveness of their destruction, whatever the medium and the method of storage.

**As regards the information of persons** If the draft articles L. 1514-1, L. 1514-2, L. 1514-3 and L. 1514-7 of the Transport Code provide that data subjects are informed of the processing of their data by the vehicle manufacturer or its representative in France, the draft articles L. 1514-4, L. 1514-5, L. 1514-6, L. 1514-8 and L. 1514-9 of the same code remain silent on this point.

acts, for example, the driver of the vehicle or the holder of the registration certificate, all the information provided for in Article 13 or 14 of the GDPR, with regard to each processing of personal data covered by the draft ordinance, provided that the latter are not anonymized before being extracted from the motorized land vehicle.

**concerning the exercise of rights** The draft ordinance does not specify the procedures for exercising the rights of individuals with regard to personal data collected via devices aimed at producing data within vehicles. The ministry indicates that the general regime provided for by



the GDPR will be applicable in this matter. , before any anonymization of their personal data, if the latter is not carried out directly in the vehicle but after extraction of the personal data from it. More specifically, the Commission emphasizes that individuals have the right to object, for reasons relating to their particular situation, to the processing of personal data concerning them when this is based on Article 6.1.e of the GDPR (when necessary for the performance of a task in the public interest or in the exercise of official authority vested in the controller) and this at any time, including prior to the implementation of processing aimed at anonymizing the data collected. Finally, in this context, the various data controllers will have to ensure the quality of the person concerned, whether it is the holder of the registration certificate or another person, in particular the person who was actually driving the vehicle during the period in question, when it is different from the holder of the registration certificate. The President M.-L.DENIS