United Nations ECE/TRANS/WP.29/2017/46

Economic and Social Council

Distr.: General
23 December 2016

Original: English

Economic Commission for Europe

Inland Transport Committee

World Forum for Harmonization of Vehicle Regulations

171st session
Geneva, 14-17 March 2017
Item 4.14 of the provisional agenda
1958 Agreement:
Proposal for amendments to the Consolidated Resolution on the Construction of Vehicles (R.E.3) submitted by the Working Parties to the World Forum for consideration

Proposal for draft guidelines on cyber security and data protection

Submitted by the Informal Working Group on Intelligent Transport Systems / Automated Driving*

The text reproduced below was prepared by the expert from Informal Working Group (IWG) on Intelligent Transport Systems / Automated Driving (ITS/AD). It is based on Working Paper ITS/AD-10-11-Rev.1, distributed during the tenth session of Informal Working group on ITS/AD. The IWG on ITS/AD is proposing the adoption of this Guideline on Cybersecurity and data protection by the World Forum for Harmonization of Vehicles Regulations (WP.29) at its March 2017 session.

* In accordance with the programme of work of the Inland Transport Committee for 2016–2017 (ECE/TRANS/254, para. 159 and ECE/TRANS/2016/28/Add.1, cluster 3.1), the World Forum will develop, harmonize and update Regulations in order to enhance the performance of vehicles. The present document is submitted in conformity with that mandate.

I. Proposal

"Guideline on cybersecurity and data protection

Guideline on measures ensuring cybersecurity and data protection of connected vehicles and vehicles with Automated Driving Technologies

1. Preamble

1.1. The digitalisation of mobility and the associated increase in the amount of data are creating new requirements to be met by vehicle safety and infrastructure and the protection of the rights and freedoms of data subjects.

1.2. As the automation and interconnectivity of driving functions increases, the issues of data encryption and cybersecurity will become more important.

1.3. Connected vehicles and vehicles with Automated Driving Technologies (ADT) thus require clear cybersecurity and data protection rules. It has to be ensured that vehicles are protected from external interference and manipulation.

1.4. This guideline is intended to present requirements to automotive manufacturers, component/system suppliers and service providers for systems to be installed in vehicles to provide a high level of cybersecurity and to ensure data protection. They can use alternative approaches where at least an equivalent level of security can be demonstrated.

1.5. This guideline is intended as interim guidance until the completion of on-going research and collaboration activities and the development of more detailed globally harmonized requirements on cybersecurity and data protection.

1.6. This guideline shall serve as a basis for the development of prescriptions in UN Regulations to ensure cybersecurity and data protection.

1.7. This guideline does not affect existing data protection legislation. This guideline is not aimed at falling short of or going beyond legal data protection regulations.

2. Scope

2.1. This guideline addresses the measures for connected vehicles and vehicles with ADT with regard to cybersecurity and data protection.

3. Definitions

3.1. (reserved)

3.2. "*Connected vehicle*" means a vehicle with a device installed designed to allow a wireless connection or communication possibly relating to automated driving technologies with external devices, cars, networks or services.

3.3. "*Cybersecurity*" means preservation of confidentiality, integrity and availability of information in the “cyberspace”, i.e. the complex environment

resulting from the interaction of people, software and services (e.g. on the Internet) by means of technology devices and networks connected to it, which does not exist in any physical form.

3.4. "*Data protection*" means a natural person's right to respect for his or her private and family life, home and communications with regard to the processing of personal data.

3.5. "*Data subject*" means an individual who is the subject of personal data (e.g. vehicle owners or drivers).

3.6. "*Data protection by default*" means a controller's obligation to implement technical and organizational measures which ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

3.7. "*Data protection by design*" means a controller's obligation to implement technical and organizational measures appropriate to the controller's processing activity which are designed to implement data protection principles with the aim of protecting the rights of data subjects by reducing the likelihood and severity of the risk to his or her private and family life, home and communications.

4. The guideline's requirements

Connected vehicles and vehicles with ADT are intended to be fitted with measures ensuring cybersecurity and data protection and shall fulfil the requirements set forth below.

4.1. General:

(a) Everyone's right to his or her privacy and communications has to be respected.

(b) Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

(c) Automotive manufacturer, component/system supplier and service providers shall respect the principles of data protection by default and data protection by design (see definitions 3.6 and 3.7).

(d) Automotive manufacturers, component/system suppliers and service providers must ensure that there is adequate protection against manipulation and misuse both of the technical structure and of the data and processes.

(e) To prevent non-authorized access to vehicles via the "cyberspace" automotive manufacturers, component/system suppliers and service providers shall ensure the secure encryption of data and communications.

(f) The system shall be accessible for verifying the measures implemented by automotive manufacturers, component/system suppliers and service providers to ensure cybersecurity and data protection by independent authorised audit.

4.2. Data protection.

4.2.1. The principle of lawful, fair and transparent processing of personal data means in particular:

(a) Respecting the identity and privacy of the data subject;

(b) Not discriminating against data subjects based on their personal data;

(c) Paying attention to the reasonable expectations of the data subjects with regard to the transparency and context of the data processing;

(d) Maintaining the integrity and trustworthiness of information technology systems and in particular not secretly manipulating data processing;

(e) Taking into account the benefit of data processing depending on the free flow of data, communication and innovation, as far as data subjects have to respect the processing of personal data with regard to the overriding general public interest;

(f) Ensuring the preservation of individual mobility data according to necessity and purpose.

4.2.2. The means of anonymization and pseudonymization techniques shall be used.

Data subjects shall be provided with comprehensive information as to what data is collected and processed in the deployment of connected vehicles and vehicles with ADT, for what purposes and by whom. Data subjects shall give their consent to the collection and processing of their data on an informed and voluntary basis.

4.2.3. The collection and processing of personal data shall be limited to data that is relevant in the context of collection. If applicable, the data subject shall have the right to withdraw his or her consent if it involves functions that are not necessary for the operation of their vehicle or for road safety.

4.2.4. In addition, appropriate technical and organizational measures and procedures to ensure that the data subject's privacy is respected shall be implemented both at the time of the determination of the means for processing and at the time of the processing. The design of data processing systems installed in vehicles shall be data protection friendly, i.e. taking data protection and cybersecurity aspects into account when planning the components ("privacy by design") as well as designing the basic factory settings accordingly ("privacy by default").

4.3. Safety.

4.3.1. Standards for the functional safety of critical electric and electronic components or systems in vehicles such as ISO 26262 shall be applied in the light of security-related requirements for connected vehicles and vehicles with ADT.

4.3.2. The connection and communication of connected vehicles and vehicles with ADT:

(a) Shall not influence internal devices and systems generating internal information necessary for the control of the vehicle without appropriate measures;

(b) Shall be designed to avoid fraudulent manipulation to the software of connected vehicles and vehicles with ADT as well as fraudulent access of the board information caused by cyber-attacks through:

(i) Wireless connection;

(ii) Wired connection via the diagnosis port, etc.

(c) Shall be equipped with measures to ensure a safe mode in case of system malfunction, e.g. by redundancy in the system.

4.3.3. When connected vehicles and vehicles with ADT detect fraudulent manipulation by a cyber-attack, the system shall warn the driver and, if appropriate, control the vehicle safely according to the above requirements.

4.4. Security.

4.4.1. The protection of connected vehicles and vehicles with ADT requires verifiable security measures according security standards (e.g. ISO 27000 series, ISO/IEC 15408).

4.4.2. Connected vehicles and vehicles with ADT shall be equipped with:

(a) Integrity protection measures assuring e.g. secure software updates;

(b) Appropriate measures to manage cryptographic keys.

4.4.3. The integrity of internal communications between controllers within connected vehicles and vehicles with ADT should be protected e.g. by authentication.

4.4.4. Online Services for remote access into connected vehicles and vehicles with ADT should have a strong mutual authentication and assure secure communication (confidential and integrity protected) between the involved entities."

II. Background information and administrative proposal

A. Background information

1. This guideline focuses on connected vehicles and vehicles with ADT.

2. The digitalization of mobility and the associated increase in the amount of data are creating new requirements to be met by vehicle safety and infrastructure and the protection of personal rights. Connected vehicles and vehicles with ADT thus require clear cybersecurity and data protection requirements.

3. Connected vehicles and vehicles with ADT are under the obligation to perform their functions safely and reliably across national borders. The rights to individual mobility data have to be regulated clearly.

4. The objective is to ensure that vehicles are protected from external interference and manipulation. The principles of global data privacy law apply to data protection.

5. For cybersecurity and data protection required steps shall be checked, e.g. system checks by external organisations.

B. Administrative proposal

6. This Guideline aims at the Construction of Vehicles and provides information on the legal texts applicable in the vehicle design, aiming the improvement of safety and the protection of the environment. The aim of this guideline is same as the aim of the Consolidated Resolution on the Construction of Vehicles (R.E.3). It is proposed to introduced the text of this guideline (Section I) as a newAnnex 6 to R.E.3.