Submitted by OICA

# OICA Comments on ITS/AD-08-05

Document No. ITS/AD-09-04
(9th ITS/AD, 22 June 2016, agenda item 3-1)

## Cybersecurity and data protection

## Part A) Focus areas for presentation at the IG ITS/AD meeting in November 2015

## Part B) Issues for discussion

## Part C) Preliminary Draft proposal for Guidelines on measures ensuring cybersecurity and data protection of connected vehicles and vehicles with automated driving technologies (ADT)

### Part A)

### I. Focus areas on automated and connected driving

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. Automated and connected driving systems thus require clear cybersecurity and data protection requirements.

Automated and connected driving systems 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.

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

For cybersecurity and data protection required steps ~~shall~~should be checked, e.g. system checks by external organisations ~~or a certification of systems~~.

**Justificaiton for delete "or a certification of systems"**
**Checks by external organisations seems acceptable, however "certification of systems" seems too strict for the nature of a guideline.**

コメントの追加 [BB1]: OICA proposes to replace "shall" with "should" throughout the document since "shall" is too strict for a guideline. Considering the situation where ISO standard also treats the terms of "shall" as mandatory requirements (not only UN Regulation but also ISO standard), the usage of "shall" in the guideline should be avoided.

書式変更: インデント：左： 10 mm

### II. Focus areas from the perspective of G7 transport ministers

Regarding cybersecurity and data protection it is stated in the declaration of the G7 Ministers of Transport and the European Commissioner for Transport on 17th of September 2015 (see Annex):

"With regard to automated driving ensuring cybersecurity and data protection are of outstanding significance and will require sustained cooperation among the G7 transport ministers and the European Commissioner for Transport."

**Part B)**

**Issues for discussion**

1. The use of clear definitions should be provided for the outline of Work item 7.
   The ToR of the IWG ITS/AD mentions eSecurity (protection against unauthorized access from outside), however it does not mention the issues related to personal data. OICA believes that issues related to personal data and data privacy are out of the regulatory scope of WP.29.

2. Evaluation of focal points by IG-ITS-AD

3. Preparation of guidelines for cybersecurity and data protection as a short-term measure.

4. At the conference of G7 transport ministers in September 2015 it was agreed to establish a working group for the coordination of the most crucial issues concerning automated driving. The IG-ITS-AD should consider the results of this working group (in particular on cybersecurity and data protection).

5. These results are expected to be available in September 2016 and should be utilized by IG-ITS-AD for further activities in developing globally harmonized specifications.

**Part C)**

**Preliminary draft proposal for Guidelines on measures ensuring cybersecurity and data protection of connected vehicles and vehicles with automated driving technologies (ADT)**

**Preamble**

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.

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

Automated and connected driving systems thus require clear cybersecurity and data protection rules. It has to be ensured that vehicles are protected from external interference and manipulation.

The guideline is intended to present requirements to automotive manufacturers and component suppliers [and service providers] for systems to be installed in vehicles to provide a high level of cybersecurity and to ensure data protection. If a manufacturer fails to comply with the requirements of the guidelines, they must guarantee security in a similar manner.

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.

Submitted by OICA

# OICA Comments on ITS/AD-08-05

Document No. ITS/AD-09-04
(9th ITS/AD, 22 June 2016, agenda item 3-1)

The guideline ~~shall~~should serve as a basis for the development of prescriptions in UNECE regulations to ensure cybersecurity and data protection.

These guidelines do not affect existing data protection legislation. These guidelines are not aimed at falling short of or going beyond legal data protection regulations.

**Scope**

This guideline addresses the measures for connected vehicles and vehicles with automated driving technologies (ADT) with regard to cybersecurity and data protection.

**1. Definitions**

1.1 Automated Driving Technologies (ADT) – definition to be added after agreement in IG-ITS-AD

1.2 Connected vehicle – A vehicle with a device installed designed to allow a wireless connection or communication [relating to automated driving technologies] with external devices, cars, networks or services.

1.3 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 on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form

1.4 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.

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

1.6 Privacy 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.

1.7 Privacy by design – means a controller's obligation to implement technical and organisational 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 for his or her private and family life, home and communications.

**2. ~~Requirements~~ / Recommendations**

This document is laid down as guideline, therefore, OICA considers that the wording "requirements" is too strict and deviate from the original purpose of the document. Also, since content of the document is described abstractly as "requirements", we are not able to verify whether it satisfies required conditions. OICA believes the proposed contents are intended as "guidelines". Hence, the usage of the term "requirements" in the guideline should be avoided.

**書式変更:** 英語（米国）

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

2.1 General

- Everyone's right to his or her privacy and communications has to be respected.
- ~~Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.~~
- ~~The manufacturer, supplier [and service providers] shall respect the principles of data protection by design and data protection by default.~~
  OICA is of the opinion that issues related to personal data / privacy are different in the '58 Agreement countries and must be met/complied with regionally anyways. Regarding the regulatory scope of WP.29, OICA suggests that the guidline contains technical related items.
- Automotive manufacturers and component 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.
- To prevent non-authorized access to vehicles, automotive manufacturers and component suppliers [and service providers] ~~shall~~should ensure the secure encryption of data and communications ~~by the use of effective information and communication technologies~~.
  - For cybersecurity ~~and data protection~~ required steps ~~shall~~should be verifiable independently by external organisations ~~or a certification of systems.~~

**コメントの追加 [BB2]:** See comments above regarding personal data protection/privacy

**コメントの追加 [BB3]:** What would be regarded as a "required step"?

2.2 Data protection

- The principle of lawful, fair and transparent processing of personal data means in particular
  - respecting the identity and privacy of the data subject,
  - not discriminating against data subjects based on their personal data,

- paying attention to the reasonable expectations of the data subjects with regard to the transparency and context of the data processing,
- maintaining the integrity and trustworthiness of information technology systems and in particular not secretly manipulating data processing,
- taking into account the benefit of data processing depending on 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.
- ensuring the preservation of individual mobility data according to necessity and purpose.

- The means of anonymization and pseudonymization techniques ~~shall~~should be used.
- Data subjects ~~shall~~should be provided with comprehensive information as to what data are collected and processed in the deployment of automated and connected driving systems, for what purposes and by whom. Data subjects ~~shall~~should give their consent to the collection and processing of their data on an informed and voluntary basis.
- The collection and processing of personal data ~~shall~~should be limited to data that is relevant in the context of collection. If applicable, the data subject ~~shall~~should 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.
- In addition, appropriate technical and organizational measures and procedures to ensure that the data subject's privacy is respected ~~shall~~should 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 such ~~shall~~should 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").

2.3 Safety

- Connected vehicles and vehicles with ADT ~~shall~~should be equipped with verifiable measures for cybersecurity taking into account the ~~latest~~ existing national and international standards.
- As there will be no longer safety without security standards for the functional safety of critical electric and electronic components or systems in vehicles such as ISO 26262 ~~shall~~should be dealt with in the light of security-related requirements for safe automated and connected driving systems for road traffic.
- The connection and communication of connected vehicles and vehicles with ADT

- ~~shall~~should not influence on internal devices and systems generating internal information necessary for the control of the vehicle with appropriate measures.
- ~~shall~~should be designed to avoid fraudulent manipulation to the software of automated driving technology as well as fraudulent access of the board information caused by cyber-attacks through;
  - wireless connection
  - wired connection via the diagnosis port, etc.
- ~~shall~~should be equipped with measures to ensure a safe mode in case of system malfunction, e.g. by redundancy in the system.

- When the system for automated driving technology detects fraudulent manipulation by a cyber-attack, the system ~~shall~~should warn the driver and control the vehicle safely according to the above requirements.

2.4 Security

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

- Connected vehicles and vehicles with ADT ~~shall~~should be equipped with

  - integrity protection measures assuring e.g. secure software updates

  - appropriate measures to manage used cryptographic keys

  The integrity of internal communications between controllers within connected vehicles should be protected by appropriate measures e.g. authentication.

  Justification for "appropriate measures"
  OICA is of the opinion that methods for protecting communications shall not be limited and that they should be prescribed in general terms. Hackers should not be given any hints. Furthermore, OICA understand that "authentication" means "message authentication" in this context, however even if that's the case, it should be considered as an example.

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

---