2.7. "*Data ~~protection~~* integrity and confidentiality" means the implementation of appropriate administrative, technical or physical means to guard against unauthorized or unlawful processing, ~~intentional~~ or accidental disclosure, modification, or destruction of data.

2.11. "*Mitigation*" means a measure that is reducing ~~modifying~~ risk.

2.14. "*Risk*" means potential that a given threat will exploit vulnerabilities of a vehicle and thereby cause harm to the organization or to an individual. ~~the effect of uncertainty on security objectives.~~

2.18. "*Threat*" means a potential cause of an unwanted incident, which may result in harm to a system or organization or individual.

**3.3.11. Access to vehicle services and functions should be controlled, in accordance with access control mechanisms and allocation of roles established in compliance with national or regional legislation, and available only to authorized parties;**

**~~3.3.12. Access to personal data of drivers and passengers should be controlled and available only to authorized parties;~~**

**3.3.13. Vehicles should log relevantaccess data, which can be used for post incident analysis and forensics.**

5.1.24. Data ~~protection~~ integrity and confidentiality best practices shall be followed for storing ~~private~~ **personal** and sensitive data

Annex A Draft proposal to introduce a Regulation on Cyber Security

Draft Regulation on Cyber Security

(…)

1.2. This Regulation is without prejudice to other UN Regulations, regional or national legislations governing the access by authorised parties to the vehicle, its data, functions and resources, and conditions of such access. It is also without prejudice to the application of national and regional legislation on privacy and the protection of natural persons with regard to the processing of their personal data.

Annex B

List of threats and corresponding mitigations

(…)

Part A. Examples of vulnerability or attack method related to the threats

|  |  |
| --- | --- |
| 32.1 | **Manipulation of ~~OEM~~ hardware**, e.g. unauthorised hardware added to a vehicle to enable "man-in-the-middle" attack  **Replacement of authorized ~~OEM~~ hardware (e.g., sensors) with unauthorised hardware.**  **Manipulation of the information collected by a sensor~~. F~~(for example, using a magnet to tamper with the Hall effect sensor connected to the gearbox) ~~(see Digital Tachograph experience)~~** |

Part B. Examples of mitigation to the threats

1. Examples of mitigation for "Back-end servers"

Examples of mitigation to the threats which are related to "Back-end servers" are listed in Table B1.

(…)

Table B8  
**Examples of mitigation to the threats which are related to "Data loss / data breach from vehicle"**

|  |
| --- |
| *Mitigation* |
| Data **integrity and confidentiality** ~~protection~~ best practices shall be followed for storing ~~private~~ **personal** and sensitive data. Example Security Controls can be found in ISO/SC27/WG5. |
|
|
|

Annex C

Examples of Security Controls related to mitigations

(…)

2. Mapping between high level mitigations given in Annex B and more detailed examples of security controls

2.1. The following table provides further detail on example security controls for the "Mitigations". The list of security controls in this table is not exhaustive. Similarly, it may not be necessary to apply all security controls listed. The selection will depend on a risk assessment and any legal, contractual, regulatory requirements in a specific Intelligent Transport Systems / Automated Driving environment.

|  |  |  |
| --- | --- | --- |
| M24 | Data **integrity and confidentiality** ~~protection~~ best practices shall be followed for storing ~~private~~ **personal** and sensitive data | 3.6 Cryptographic security  83. Monitoring  3.9 System design   Systems are designed so that end-users can efficiently and appropriately access, delete and manage their personal data   Define measures to ensure secure deletion of user data in case of a change of ownership  **Possibility to define rules for the management of the personal data**  3.10 Software security  3.13 Information exchange |

3. Further information on Security Controls

(…)

3.5. Access control

3.5.1. The following points may apply:

3.5.1.1. Points related to "Access control mechanisms"

- Establish trust boundaries and access controls

- Apply least **privilege** ~~access~~ principle **so that that users, systems, and processes only have access to resources (networks, systems, and files) that are absolutely necessary to perform their function assigned in compliance with national or regional legislation**. ~~to minimise risk~~

(…)