Feedback on FIA's proposal for cyber security guideline (ITS/AD-08-05)

No.	Position	Original	FIA Proposal	Feedback on Proposal
1	Part A-I Para. 1	Automated and connected driving systems thus require clear cybersecurity and data protection requirements.	FIA fully supports the Basic Principles on the protection of personal rights and cybersecurity. FIA likes to lay down these principles as a requirement for the technical design of an automated and connected vehicle.	A regulation with clear requirements is a long-term goal of the development of these guidelines at second step work.
2	Part A-I Para. 3	The principles of general data privacy law apply to data protection	The principles of strongest data privacy law apply to data protection	More proper wording is "global" instead of "strongest"
3	Part A-II Para. 4	For cybersecurity and data protection required steps shall be checked, e.g. system checks by external organisations or a certification of systems.	FIA fully supports this request. The methodology of Common Criteria would allow such a certification on a technology neutral basis	----------
4	Part A-II Title	II. Focus areas from the perspective of G7 transport ministers	FIA fully supports the G7 requirements	----------
5	Part B Item 3	Preparation of guidelines for cybersecurity and data protection as a short-term measure.	FIA offers to participate actively in this work.	----------
6	Part C Preamble Para. 4	If a manufacturer fails to comply with the requirements of the guidelines, they must guarantee security in a similar manner.	FIA supports this process and proposes to define a security target that must be met by all stakeholders and all technical solutions.	----------

No.	Position	Original	FIA Proposal	Feedback on Proposal
7	Part C Preamble Para. 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.	FIA fully supports an interim solution, as cyber attacks on vehicles are already a reality in the current fleet.	----------
8	Part C Definition 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.	While technical measures can be checked during type approval, we need more information on organizational measures and how secure they are	Differentiation of organizational measures has to be performed during the process of future development of these draft guidelines. It must be possible to verify also organizational measures.
9	Part C Definition 1.8	(Item that is not in the original	Freedom of choice – means a controller´s obligation, that the data subject can start/stop the datatransfer from his vehicle, but also redirect the datatransfer to other service providers of the vehicle owner´s choice	Ask FIA for intention of the new definition item proposal

No.	Position	Original	FIA Proposal	Feedback on Proposal
10	Part C Requirements/ Recommendation General Item 3	The manufacturer, supplier [and service providers] shall respect the principles of data protection by design and data protection by default.	FIA needs further clarification on what the authors mean by data protection by default	See modified definitions 1.6 and 1.7
11	Part C Requirements/ Recommendation General Item 4	Automotive manufacturer and component suppliers [and service providers] must ensure that there is adequate protection agair manipulation and misuse both of the technical structure and of the data and processes.	FIA "adequate" needs to be defined	Definition for "adequate" is a second step work.
12	Part C Requirements/ Recommendation General Item 5	To prevent non-authorized access to vehicles, automotive manufacturers and component suppliers [and service providers] shall ensure the secure encryption of data and communications by the use of effective information and communication technologies.	FIA; to ensure an open market, there should also be me measures for an authorized access, see 1.8 "freedom of choice"	Measures on authorized access are expandable because the objective of the guidelines is the protection against unauthorized access. Authorized access is beyond the scope of the document.
13	Part C Requirements/ Recommendation General Item 6	For cybersecurity and data protection required steps shall be verifiable independently by external organisations or a certification of systems.	FIA fully supports this request. The methodology of Common Criteria would allow such a certification on a technology neutral basis, see also Part A) on page 1	----------
14	Part C 2.2 Data protection Item 2	The means of anonymization and pseudonymization techniques shall be used.	FIA fully supports the pseudonymization of personal data	----------

No.	Position	Original	FIA Proposal	Feedback on Proposal
15	Part C 2.2 Data protection Item 4	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.	FIA: "Not applicable" should only be used in legally anchored data transmission, e.g. eCall 112. In all other cases the data subject must have the right to withdraw his consent.	"If applicable" makes sense because cases are conceivable where the withdrawal of consent may compromise the safe operation of the vehicle.
16	Part C 2.4 Security Item 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).	FIA regards the methodology of common criteria the most proper measure for cyber security and fully supports this requirement.	----------
17	Part C 2.4 Security Item 4	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.	FIA supports an open and secure access to in-vehicle-data. As IT develops faster than vehicles, the software in the vehicle should be updated, if cyber attacks took successfully place.	----------