

Stakeholder Feedback to  
Legislative and key action plan for transport automation  
VN/ 15033/ 2019-LVM-90

15.01.2021

## **A. SUMMARY**

1. Connectivity, algorithmic transparency, cyber security:
  - Certification by a third party - could lead to possible conflicts of interest; countermeasures shall be evaluated as part of the plan
  - Data-sharing and free data exchange - adds costs, and if some data is required to be shared who will decide and define that
  - Creates additional responsibilities and liabilities for stakeholders (private business)
  - Cyber security and privacy issues are unresolved and not identified in the plan
  - How software system in vehicles training data can be tested for discrimination - what are current criteria for data selection as we use real-time recorded data, and even this use is not clarified by privacy authorities?
  - Transparency to authorities and third parties, on the other hand no need to reveal IPR - who defines and decides this
  
2. More detail and clarity on the overall schedule and development of the AD roadmap, for instance:
  - a) What is the current role of Finnish authorities as it is perceived at UNECE or EU - do we actually have a position to play a leading role in developing regulation and will anyone follow our national practices or should we better focus on following the major trend that finds support throughout global market stakeholders?
  - b) Should we follow general automotive industry standards or expect that autonomous systems standards will be drastically different?

c) What means "driverless" in the context of the current plan - does it actually mean that a safety driver has to be inside the vehicle for the foreseeable future? And if remote centre operator is available option, how exactly this corresponds with, for instance, currently adopted German legislation in this area; do we have a conflict (provided that German market is one of the most influential in EU in automotive industry and Finland does not have an automotive industry)

d) What is the actual nature of the testing tracks discussed in the plan: will they be built for anyone to use on certain terms for any testing or will they be used specifically for the technology audit/validation?

3. More information and clarity hoped for on how to be involved in the stakeholders' process and discussions

4. Main focus and responsibility to be provided/assumed by the national authorities - how to ensure it does not lead to unnecessary problems in international and cross-border collaboration and operation and creates barriers to entering other national markets within the EU or globally?

5. Conflicting objectives and actions; better coordination between different topics of the plan is advisable (e.g. goal is to make legislation easier for piloting, but at the same time requiring fail-safe mechanisms for safety - is it a final product or experimental development and testing requirement?)

## **B. Detailed comments and explanation by topic**

### **1. GDPR/personal data processing**

- **Unclear requirements and practices** for the **personal (video) data exchange** in various projects. In publicly funded EU project set goals/results required data exchanges (including video images of people and vehicles) for the benefit of the digital data economy and related products' development (5G, NeutralHost/LuxTurrim project), however, all 26 project participants experienced difficulties with defining their status (data controller/processor/joint controller), responsibilities towards authorities, data subjects and members of the same consortium. **Indecisiveness, lack of common understanding, unclear position of authorities** on the matter and connected delays may **impair full data**

**exchange** and **exploration** of the full potential of the technology for the development of the new solutions and products in reaching targets of the EU project, and potential of various stakeholders' cooperation in this area. Project, among others, had a target of testing data exchange via operator centre, which will not be possible if conditions are not created for sufficient mutual protection and compliance of all parties with video data exchange and protection.

- **Different national practices of data protection authorities** with respect to video data collected by autonomous vehicles during testing. E.g. regulation in this area is more developed in Norway (Datatilsynet) than in Finland (Tietosuoja), even though both are based on the same initial sources: GDPR and EDPB Guidelines 3/2019 on processing of personal data through video devices. **Lack of transparency** and **clarity on cooperation between Data Protection authorities in EU** countries in cases where service providers (like our company) is located in Finland and the customer/MaaS provider operating vehicles with our ADAS system collects and transmits vehicle data (including video data recorded by vehicle cameras) across the border.
- In another publicly funded EU project, it is a mandatory requirement to transmit audio between passenger and remote operator. In the light of the recent fines in Finnish market by the Data Protection Authority for recording audio as "excessive data collection", it is unclear how this requirement can be legally fulfilled by the project participants without creating serious compliance risk for the participants. GDPR issues are not clarified or coordinated in relation to autonomous driving and there is no consistency with the public projects requirements and GDPR requirements.

## **2. Open interfaces and free technical data exchange**

- will create additional cost on market actors (vehicle owners/operators), obligations (quality, security) and privacy issues for those who will be forced (incentivised?) to share data
- It seems that actual market actors will be forced to share dynamic real time data to create/update digital infrastructure – who and how will define terms of this activity and compensation of private players costs?
- As dynamic traffic information is collected by vehicles (very limited in Finland) – what is the plan for the information collection and exchange to cover the whole territory?

### **3. Utilization of data from the use cases**

- how this will be handled and who will define the process?
- Provided that emphasis is on the data quality, production responsibility, access rights and sharing – it all generates extensive costs, privacy and security issues for the vehicle owners/operators – how this issue can be handled in reality?

### **4. Ethical AI**

- Who will define criteria for AI training data and impact assessment? Will stakeholders be involved in this process and if so, which actors?
- Training Data may vary between various AI applications – will vehicle AI quality data have its own rules or general with other AI applications?

How will this be coordinated in the EU and internationally?

- As in training personal (video) data is used, how this can be regulated under GDPR as currently there is a gap and unclarity on this topic?
- Personal data requires limited access and storage – additional challenge to be addressed, who will handle these issues with data protection authorities?

### **5. Algorithmic transparency vs. trade secrets**

- How sufficient IPR protection is planned to be achieved? Is it even possible to describe the specifics of the system without revealing trade secrets as all existing ADS are different and function differently and this information is impossible to come across on the detailed level? It is really that the whole functioning of the system shall be described or just the safety aspects? Or how vehicle sensor system can be validated in terms of non-discrimination?
- Who will participate in the criteria defining and how this will be coordinated within the EU and internationally?
- How issues of confidentiality will be handled (e.g. officials can change jobs into the private sector and carry collected confidential information without repercussions; how sufficient expert level to understand underlying issues will be measured and achieved; is log-data, i.e. personal data, really necessary to understand the system functionality?
- How will the GDPR aspect of it be handled (as a big amount of data is video data and some of it audio)?

- Where will be the difference of "algorithmic transparency" between what the authorities/auditing companies have to assess and the public has to know?

## 6. Regulation and Market Barriers for testing and operation of technology

- Differences in the **local regulation** of the autonomous vehicles' **testing**. Acquiring testing registration plates, local insurance and similar operations in Norway require establishing a local branch, acquiring local transportation insurance and a number of other requirements that significantly burden and delay the process.
- Unclear situation regarding vehicle insurance – it seems to be attached to the national registration plates and not to the vehicle itself. Therefore, insurance acquired in Finland for one vehicle is no longer valid, when applying for testing license plates in Norway and a new insurance is required alongside the new license plates. Only a local company can apply for such permits (restricting competition?); a foreign company from another Nordic country is required to establish a branch office with a local representative, that in turn creates a significant amount of additional administrative, financial and economic barriers to AV testing across borders. In one of our cases, we had to find and hire a local operating company leasing vehicles from us, applying for the permits and securing insurance, where that company will be the sole beneficiary. This renders our Finnish company being not included in any motor insurance (mandatory or comprehensive) regarding our own vehicles, temporarily tested in Norway.
- *Wider national regulation and diversified criteria:*
  - i) will create an issue for cross-border operations and product sales – how this can be mitigated for Finnish developers (and for foreign automotive companies entering Finnish market)?
  - ii) How developers from one EU state will be able to meet requirements from other EU states? Who and how will coordinate this process on EU and international levels? Especially, if every nation will adopt their own market requirements
  - iii) already exist in the national liability regimes, including difference in the product liability enforcement process
- *National Ethical AI regulation:*
  - i) Does it make sense for each EU nation to have its own ethical AI guidelines?
  - ii) How varying national requirements will be mitigated to remove market obstacles for cross-border trade and operation?

- How will the process of technology neutral solution be coordinated nationally with the EU process regarding Product Liability regime adaptation?

## 7. Liability

- Issues of **liability** for **damages caused to third parties** (passengers, pedestrians, other vehicles and road property) during the testing remain open due to recent preparatory works on modifications of the Product Liability Directive. "Manufacturer" (vehicle producer/system developer) may be the same legal entity or different stakeholders, where developer usually an SME and vehicle producer is an OEM/tier 1. Tested AV is not represented as a ready for the market deployment product, however, testing is sanctioned in all EU countries. Yet, in theory it is placed on the market when tested and all parties act in the circumstances of legal uncertainty, taking uncalculated risks. Shall the damage take place, provided actual compensation takes place in accordance with the national rules on liability, it is difficult to foresee if the victim gets prompt compensation, who will be paying, if the driver will not be negligent, and resulting dispute between vehicle manufacturer and software developer regarding whose defect caused the damage may extend for years, eventually putting SME out of business due to extensive legal fees only.
- Already now many customers would like to discuss "standard of care" we apply in our activity. With autonomous vehicles not having their specific ISO standards and industrial practices, it is difficult to anticipate how to establish the state of the art. In the light of the recent challenging of the "state of the art defence" applicability to the autonomous vehicles, along with absence of any specific standards, it makes it impossible to define threshold of safety and project commercialisation of the technology
- It is not clear what is the current state of the art, the benchmark for autonomous technology development - shall developers follow automotive industry standards, software industry standards, both or expect drastically different standards for safety and validation procedures? Changing to risk-based and goal-based requirements from the detailed technical sounds great, but how can it be implemented in reality in comparison to existing ISO 62626, for instance?



- Freedom of building technologically neutral solutions – who will be liable for the choices made: what operator is best positioned to carry the risk?

## **8. Other market- and infrastructure-related**

Support for public bus mobility services market creation

- What kind of measures are anticipated and who are the actors?

Physical infrastructure, specifically electricity supply

- Plan did not mention charging facilities for EVs along motorways, suburban areas – how this will be incorporated into the Plan, if at all?

Sincerely yours,

Sensible 4 Oy team