39th International Conference of Data Protection and Privacy Commissioners

Hong Kong, 25-29 September 2017

Resolution on Data Protection in Automated and Connected Vehicles

Proposer:

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

The Federal Commissioner for Data Protection and Freedom of Information, Germany

Co-Sponsors:

- **Commission de la Protection de la Vie Privée**
  Belgian Data Protection Authority
- **Commission Nationale de l'Informatique et des Libertés (CNIL)**
  French Data Protection Authority
- **The Privacy Commissioner for Personal Data, Hong Kong, China**
- **Garante per la protezione dei dati personali**
  Italian Data Protection Authority
- **Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)**
  National Institute for Transparency, Access to Information and Personal Data Protection, Mexico
- **Office of the Privacy Commissioner, New Zealand**
- **Informacijski pooblaščenec Republike Slovenije**
  Information Commissioner of the Republic of Slovenia
- **Préposé fédéral à la protection des données et à la transparence**
  Swiss Data Protection Authority
- **Information Commissioner's Office, United Kingdom**

Recognizing that automated and connected vehicles may offer significant benefits for users by providing enhanced levels of usability or convenience, as well as for the general public by

improving traffic efficiency and safety of vehicle drivers and their passengers, other road users and pedestrians;

Highlighting the rapid advancement of vehicle automation and connected vehicle technologies allowing the development and introduction of new and innovative products, devices or telematics services, which in many cases will include the collection and processing of personal data due to the wide variety of sensors installed in them, thus evoking new challenges to the rights to the protection of personal data and privacy of users especially when regarding the multiple scenarios where vehicles might be used by many persons;

Noting the Declaration of the G7 Ministers of Transport and the European Commissioner for Transport at their meeting in Cagliari, Italy, on 21-22 June 2017[1] which recognizes the necessity to follow relevant existing guidelines on cyber security and data protection and encourages all actors to assess how the necessary data can be used for the development of services and applications which improve safety and traffic conditions while respecting consumers' cybersecurity and privacy interests;

Noting the Declaration of the G20 Ministers responsible for the Digital Economy at their meeting in Düsseldorf, Germany on 6-7 April 2017 on Shaping Digitalization for an Interconnected World[2] which recognizes the necessity to strengthen trust in the digital economy by respecting legal frameworks for privacy and data protection and strengthening security in the use of information and communication technology as well as transparency and consumer protection;

Concerned about the possible lack of available information, user choice, data control and valid consent mechanisms for vehicle owners, drivers and their passengers and other road users and pedestrians to control the access to and use of vehicle and driving-related data;

Observing the development of different technologies for cooperative intelligent transportation systems where vehicles share their positional and kinematic data by continuously broadcasting information to other vehicles (v2v), transportation infrastructure (v2i) or other third party's entities (v2x) to gather an overall picture of the current traffic situation in order to foster traffic safety and efficiency;

Concerned that unrestricted and indiscriminate dissemination of data by the vehicles in the context of v2v, v2i and v2x communication might lead to illegitimate use, unauthorized access to, or further processing of, the drivers', passengers' or other individuals' personal data by third parties;

---

[1] http://www.g7italy.it/sites/default/files/documents/Final Declaration_0.pdf

[2] https://www.bmwi.de/Redaktion/DE/Downloads/G/g20-digital-economy-ministerial-declaration-english-version.pdf?__blob=publicationFile&v=12

Noting on the other hand that technologies for cooperative intelligent transportation systems must be designed in a way that allows for the traceability and authentication of vehicles, thereby duly considering the principles of privacy by design and privacy by default;

Acknowledging that the developers of the different technologies for cooperative intelligent transportation systems are aware of privacy risks emerging from such technologies and have taken considerable efforts to minimize those risks by reducing the amount of personal data and by making the identification of data subjects difficult;

Noting that a comprehensive collection of data shared within a connected vehicles system including cooperative intelligent transportation system, may not only lead to the accumulation of individuals' movement profiles, but could also generate vast amounts of data on the evaluation of driving behaviors, which may prove to be valuable information for certain entities, e. g. motor insurance companies, vehicle manufacturers, advertisers as well as law and traffic enforcement agencies, particularly when data will be personalized, e.g. by utilizing any broadcast vehicle identifiers;

Mentioning best practice solutions in pay television broadcasting and digital police radio to restrict access to broadcasted information to authorized recipients;

Observing that data protection and privacy commissioners provide specific guidance on privacy rules applicable to automated and connected vehicles' related processing or solutions;

Noting that the World Forum for Harmonization of Vehicle Regulations has now included guidelines on cyber security and data protection in its consolidated resolution on the construction of vehicles (R.E.3)[3] as annex 6;

Affirming the requirements laid down in part I section 4 of the aforementioned guidelines on cyber security and data protection which include giving consideration to the concepts of privacy by design and privacy by default;

Reaffirming the resolution on Privacy by Design[4] adopted by the 32th Conference of Data Protection and Privacy Commissioners 2010 in Jerusalem, the resolution on profiling[5] adopted by the 35th International Conference of Data Protection and Privacy Commissioners 2013 in Warsaw as well as the resolution on big data adopted by the 36th International Conference 2014 in Fort Balaclava, Mauritius [6];

[3] https://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29resolutions/ECE-TRANS-WP.29-78r5e.pdf

[4] https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf

[5] https://icdppc.org/wp-content/uploads/2015/02/Profiling-resolution2.pdf

[6] https://icdppc.org/wp-content/uploads/2015/2/Resolution-Big-Data.pdf

The 39th International Conference of Data Protection and Privacy Commissioners calls upon all relevant parties involved, particularly

- **standardization bodies,**
- **public authorities,**
- **vehicle and equipment manufacturers,**
- **personal transportation services and car rental providers,**
- **providers of data driven services, such as e.g. speech recognition, navigation, remote maintenance or motor insurance telematics services,**

to fully respect the users´ rights to the protection of their personal data and privacy and to sufficiently take this into account at every stage of the creation and development of new devices or services.

Thus, the parties mentioned above are seriously urged to

1. give data subjects comprehensive information as to what data is collected and processed in the deployment of connected vehicles, for what purposes and by whom,
2. utilize anonymization measures to minimize the amount of personal data, or to use pseudonymization when not feasible,
3. keep personal data no longer than necessary in relation to the legitimate purpose for which they are processed, for further compatible purposes, or in accordance with law or with consent, and to delete them after this period,
4. provide technical means to erase personal data when a vehicle is sold or returned to its owner,
5. provide granular and easy to use privacy controls for vehicle users enabling them to, where appropriate, grant or withhold access to different data categories in vehicles,
6. provide technical means for vehicle users to restrict the collection of data,
7. provide secure data storage devices that put vehicle users in full control regarding the access to the data collected by their vehicles,
8. provide technical measures for secure online-communication components that protect against cyber-attacks and prevent unauthorized access to and interception of personal data,
9. develop and implement technologies for cooperative intelligent transportation systems in ways that

a. prevent unauthorized access to and interception of personal data collected by vehicles (v2v), transportation infrastructure (v2i) or other third party's entities (v2x),

b. enable vehicle users to inhibit the sharing of positional and kinematic data while still receiving road hazard warnings,

c. provide safeguards against unlawful tracking and tracing of drivers,

d. ensure the security mechanisms of v2v, v2i and v2x communication during authentication processes do not pose additional risks to privacy and personal data and

e. limit the possibility of illegitimate vehicle tracking and driver identification.

10. respect the principles of privacy by default and privacy by design, by providing technical and organizational measures and procedures to ensure that the data subject's privacy is respected, both when determining the means of the processing and at when processing the data,

11. develop privacy preserving technologies and architectures that favorably process personal data onboard,

12. guarantee the self-learning algorithms needed for automated and connected cars are made transparent in their functionality and have been subject to prior assessment by an independent body in order to reduce the risk of discriminatory automated decisions,

13. provide vehicle users with privacy-friendly driving modes with default settings,

14. undertake data protection impact assessments for new, innovative or risky development or implementation of these technologies,

15. promote the respect of the personal data privacy of vehicle users by responsible processing of their personal data, and giving due consideration to the potential harm that may be caused to the vehicle users as a result of the processing and use and

16. enter into a dialogue with the data protection and privacy commissioners to develop compliance tools to accompany and provide legal certainty to connected vehicles' related processing.