ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN

WP 252

Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS)

Adopted on 4 October 2017

Table of content

Table of content

1 Introduction

The document “Processing personal data in the context of C-ITS" drafted by the Data Protection and Privacy Working Group of the Cooperative Intelligent Transport Systems (C-ITS) platform was formally submitted to the Article 29 Working Party on 10 July 2017.

The C-ITS platform is an initiative of Directorate for Transport and Mobility of the European Commission, which started at the end of 2014 with the creation of specialized working groups, each addressing various aspects of C-ITS deployment, ranging from security, to technical standardization, to data protection.

The scope of the document is to provide background information on the processing of personal data in the context of C-ITS, and to seek guidance from the Article 29 Working Party in order to enhance the level of data protection within these new types of application.

The Article 29 Working Party has been invited by the Commission to attend with its delegates a number of preparatory meetings, before delivering the present opinion.

The Article 29 Working Party appreciates the opportunity to get involved in the discussion with the relevant stakeholders since the early stage of development of this new technological concept, and will accordingly raise some points of concerns relating to the General Data Protection Regulation (GDPR) that will be the legal framework in force at the time of deployment of the C-ITS solution.

The Article 29 Working Party welcomes the recent resolution on Data Protection in Automated and Connected Vehicles of the ICDPPC Hong Kong, 25-29 September 2017 affirming the requirements laid down therein.

2 The C-ITS concept

C-ITS is a peer-to-peer solution for the exchange of data between vehicles and other road infrastructural facilities (traffic signs or other transmitting/receiving base stations) without the intervention of a network operator.

The concept of the system is that peers can directly inform each other about their own status (elaborating data gathered by sensors with which they are equipped), receiving in return similar information, and thus allowing the creation of an overview (for each peer) of the status of the environment surrounding the vehicle or infrastructural facility. Based on these communications, the expectation is that better predictions about the traffic situations can be made and accident prevention can be improved.

C-ITS is based on continuous broadcasting. It creates ad-hoc communications and does not require the establishment of permanent communication or links between the peers.

Two types of messages are exchanged in the context of C-ITS: the so-called Cooperative Awareness Messages (CAM), broadcasted with continuity and containing kinematic data and the dimensions of the vehicle, and the Decentralised Environmental Notification Messages (DENM), sent in addition to the CAM messages only upon the occurrence of specific events (like accidents) for urgent emergency situations, and containing location information about the event.

CAM and DENM messages include cryptographic signatures, guaranteeing the receiving party that the messages are sent by a trustable sender. The distribution of certificates among the peers is made using a Public Key Infrastructure (PKI) architecture. The PKI is a governance structure in which each certificate at a specific time is uniquely associated to a vehicle. The certificate shows that it is recognised by the system and can be trusted.

The European Commission in its C-ITS strategy has already identified a number of use cases for initial deployment (day-one applications). These cases, as specified in the document from the C-ITS Data Protection and Privacy Working Group are mostly related to informational functionalities (such as road works warnings, weather conditions etc.). The driver in these use cases remains in full control of the vehicle and is liable for the actions of the vehicle. In the long term, and with an enhanced level of automation, the impact of C-ITS is expected to increase, as the system might gradually take over driving decisions from the driver.

The Article 29 Working Party will solely focus on these initial capabilities of C-ITS applications. When higher levels of automation are implemented, this will raise new, highly relevant questions about the impact on freedom and rights of EU citizens. The Article 29 Working Party, and in time the European Data Protection Board, will assess these issues in a later stage. The Article 29 Working Party takes the opportunity to encourage a timely dialogue between the relevant stakeholders on the data protection implications of these evolutionary scenarios, by also considering the difficult ethical questions raised by such a new, in-depth intervention in traditionally human-managed actions.

3 Summary of C-ITS working document

3.1 Personal data

The Data Protection and Privacy Working Group of the Cooperative Intelligent Transport Systems recognizes that the broadcast messages exchanged by the vehicles are personal data. Essentially, this conclusion stems from two observations: 1) the messages contain authorisation certificates, issued by the PKI, univocally associated to the sender; 2) the messages contain heading, timestamp, location data and the dimensions of the vehicle.

The document qualifies the mechanism in place to exchange CAM and DENM messages with their digital certificates as a processing of pseudonymized data, arguing that additional information (the association between the certificate holder and the data of the vehicle) is kept separate from the data utilizer (this information is held by the certification authorities). Thus according to art. 4(5) of GDPR additional information would be needed in order to identify data subjects. This is why the document claims that art. 11 of the GDPR (processing which does not require identification) would have to apply. However the document does not address the processing carried out by the certification authorities and does not give technical details on the PKI infrastructure, which are critical to ensure that the exchanged data will be practically pseudonymous.

3.2 Legal grounds

The Data Protection and Privacy Working Group of the C-ITS platform concludes that lawfulness of the processing might not be grounded only in one, but on a combination of two or more legal bases, taking into account the timing and with a view to deploying the new

technology in 2019. As a summary, the C-ITS Working Group considers that the possible appropriate legal bases, or combination of them, having in mind the nature of the day-one applications provided, might be:

- Public interests (art 6(1)e GDPR)
- Performance of a contract (art 6(1)b GDPR)
- Consent (art 6(1)a GDPR)
- Legitimate interest (art 6(1)f GDPR)

The C-ITS Working Group notes that in order to apply public interest as legal ground, the necessity for this processing must be laid down in a national or EU law. This could be envisaged in implementing the EU strategy for road safety, transport efficiency and environmental sustainability. The ITS Directive 2010/40/EU allows the European Commission to adopt binding specifications in this field via delegated acts. The C-ITS Working Group considers mandatory deployment of C-ITS as an option, but not for the initial deployment in 2019.

The C-ITS Working Group has considered the option of processing personal data where this is necessary to perform a contract to which the data subject is party. According to the conclusions reached by the C-ITS Working Group, the applicability of this legal basis might not be general. The reliance on this legal ground may be possible in specific scenarios, for instance when the data subject actually does have a contract with a private road operator to be able to drive on that road. The C-ITS Working Group notes that there is a chain of actors involved in the C-ITS framework (car manufacturers, software developers, road managers). They may be joint controllers as defined in art. 26 of the GDPR. In order to be able to rely on the legal basis of necessity to perform a contract, an assessment is required of the roles of the various entities in relation to purposes and means.

With regard to the legal ground of consent, the C-ITS Working Group elaborates on the technical constraints posed by the broadcasting nature of the communications. In the C-ITS context, the actors that fulfil the role of data controllers might not have a direct one-to-one relationship with the data subject. The data subject is not and cannot be aware of all recipients of his messages, given the way the standard is conceived[1]. However, the C-ITS Working Group suggests the possibility to attach markers to the broadcasted CAM and DENM messages, where users' preferences can be coded.

The C-ITS Working Group has also considered the processing for the purpose of the legitimate interests pursued by the controller. In order to be able to rely on this legal ground, the data controller must ensure that the processing does not override the interests or fundamental rights and freedoms of the data subject. Many constraints, as explicitly recognized in the document, stand in the way of the applicability of this legal basis. Primarily, the need to identify whose interest is pursued in the C-ITS chain of responsibilities, the performance of potentially separate balancing tests by each of the actors involved, depending on their roles, and secondarily, the implementation of additional specific safeguards to limit undue impact on data subjects.

[1] ETSI EN 302 637-2 'Intelligent Transport Systems "ITS; Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service' and ETSI EN 302 637-3 'Intelligent Transport Systems ITS; Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralised Environmental Notification Basic Service'

4. Opinion of the Article 29 Working Party

4.1 The legal framework

The initial deployment of the Cooperative Intelligent Transport Systems is envisaged for 2019. The relevant legal framework for the processing of personal data in relation to C-ITS is therefore Regulation (EU) 2016/679 of the European Parliament and of the Council "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data" (GDPR) that has entered into force on 25 May 2016 and will be applicable law by 25 May 2018.

Additionally, in the future the new ePrivacy Regulation may become relevant. According to the proposal from the European Commission (COM(2017)10) [2], machine to machine communications should fall under the scope of this Regulation.

4.2 Personal data / identification of data subjects

The C-ITS Working Group has correctly identified that data transmitted via C-ITS is personal data, since it relates to identified or identifiable data subjects. The data subjects can be identified in various ways. First, by the certificates they are provided by the PKI, since those certificates will be unique by design, in order to disambiguate the vehicle in which they are installed. Second, by the location data themselves, since the power of identification of location data is well known[3]: just a few points in a path are enough to single out an individual in a population with a high degree of precision, taking into account the mostly regular patterns of people's mobility.

This is especially true for CAM messages. DENM messages also include authorisation tickets and the data describing a specific event. Depending on the way the event occurs (e.g. the sparsity of the area, the peculiar daytime or the event chain dynamics), these messages may also make the data subject identifiable.

On the applicability of art. 11 of the GDPR, the Article 29 Working Party would like to raise the following concerns. Article 11 states that there are processing operations for which the identification of a data subject is not necessary, or no longer necessary, and the controller shall not be obliged to identify the data subject for the sole purpose of complying with the GDPR. This article should be interpreted as a way to enforce 'genuine' data minimization, without however hindering the exercise of data subjects' rights. Exercise of these rights must be made possible with the help of 'additional information' provided by the data subject. By invoking art. 11 of the GDPR without specifying what additional data are necessary to enable identification of the data subjects, the exercise of data subjects rights (access, rectification, portability, etc.) is *de facto* prevented. However, pseudonymized data are personal data by definition (see art. 4 GDPR), in that they are data relating to an identifiable individual (see, in particular, Recital 26 GDPR).

[2] European Commission legislative proposal COM(2017)10 concerning the respect for private life and protection of personal data in electronic communications (the e-Privacy Regulation), january 2017. See also Opinion WP247 of the Article 29 Working Party, URL: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103.
[3] Article 29 Working Party, WP X, Opinion 05/2014 on Anonymisation Techniques.

Therefore, the Article 29 Working Party calls for proposals from the C-ITS WG on the concept of "additional information" that can be provided in the context of this new service to make this provision effective, taking into account for instance specific vehicle data, or the highly identifiable nature of location data. The Working Party rejects any interpretation of Article 11 aiming at reducing the responsibility of the controller(s) for compliance with data protection obligations.

The personal data processed through C-ITS may also include special categories of data as defined in art. 10 of the GDPR, related to signal violation (for instance the "signal violation/intersection safety" in the document). These special categories of data can be processed in C-ITS and broadcasted to other vehicles. Art. 10 of the GDPR specifies that data relating to criminal convictions and offences may only be processed under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. As a consequence the day-one applications should be modified to prevent collection and broadcast of any information that might fall under Article 10.

The Working Party sees several technical possibilities to minimize the risks of reidentification.

Firstly, the issuing policy of PKI certificates can be improved. As long as a certificate is valid, a vehicle can be identified and tracked, and short range tracking is an important C-ITS design component. The short range tracking allows for a tight causal connection between road conditions and the vehicles driving in that area, and is therefore considered necessary to enable the system and make applications work. In order to prevent long term tracking, which is not essential for road safety, authorization tickets are changed over time. While the C-ITS Working Group underlines the need for a low frequency with which authorization tickets are changed, in order to limit certificate consumption and not to frustrate easy identification of dangers and warnings about nearby drivers, the Article 29 Working Party recommends to carefully assess the possibilities for a higher frequency, in order to limit the risks of long term tracking.

Secondly, the frequency of broadcasting of CAM messages needs to be adjusted.
According to the proposed frequency settings of CAM messages, it would be possible to track vehicles in the range of a few meters. This can be done for example if different segments of very dense sequences of time-referenced dots, which can be located for instance on a map, are "coloured" differently by a specific certificate (assuming that each certificate visually gets a different colour). The assertion made by the C-ITS Working Group in the document, that "colouring differently" (i.e. attaching different certificates to) these segments on a map would prevent an observer from reconstructing the whole path of a vehicle, is questionable. Mobility data are inherently and strongly correlated, and very repetitive for most drivers, and the exercise of reconciling apparently disjointed segments in an end-to-end path should not be considered unreasonable for an attacker with the means and the motivation. Furthermore, when a vehicle changes its certificate it will still be possible to link the old and the new certificate: any other vehicle in the vicinity of the vehicle changing its certificate will be able to witness the disappearance of the old certificate and the appearance of the new certificate, and thus will be able to link them together. The C-ITS Working Group should address this issue in order to prevent such correlations.

Thirdly, the Article 29 Working Party underlines the importance of the data minimization principle to mitigate the risks of reidentification, also by means of the application of remedies

such as generalization or noise injection[4]. Such remedies can be engineered in order not to affect the overall picture of the environmental status and the possibility to spot a new danger, while limiting unnecessary exposure or long term tracking of the driver. Specific attention should be given to generalization or noise injection of the static properties of vehicles to minimize the risk of tracking by fingerprinting vehicle properties.

4.3 Privacy Risks

The Article 29 Working Party recognises that the concept behind C-ITS may bring benefits for drivers by providing enhanced levels of usability and environmental awareness, and for the general public by improving road safety and protecting the safety of other drivers and pedestrians. Nevertheless, the Article 29 Working Party highlights that the large scale deployment of this new technology, which will entail the collection and processing of unprecedented amounts of location data of individuals in Europe, poses new challenges to the fundamental rights and to the protection of personal data and privacy both of users and of other individuals that will possibly be affected.

First of all, C-ITS by concept will make exposable what we were not used to disclose: where we drive and the way we drive. By means of the transmitting and receiving capabilities of the vehicles, these intimate pieces of information will be publically broadcasted to any nearby vehicle. This is a form of distributed permanent behavioural tracking which can generate an uncomfortable sense of stealthy surveillance.

Lack of transparency is another major privacy risk. Through their vehicles, users will become continuous broadcasters. They must be fully aware of the scope of the processing, of the other peers with whom they exchange data in the C-ITS environment (other vehicles, car manufacturers, roads managers, other public or private parties) and how they process these data.

The choice of broadcast among peers to distribute messages, instead of one to one communications, poses another challenge: messages can be received by an unrestricted number of entities, whose intentions and technological capacity are not, and cannot be known to the sender. This causes an informational asymmetry between the senders and the other peers (receivers) of the C-ITS. This asymmetry needs to be rebalanced with a higher level of control on the personal data.

Kinematic and location data will be highly valuable to a number of interested parties with diverse intentions and purposes, ranging from advertisers to car manufacturers and insurance companies. Unrestricted and indiscriminate access to data shared within C-ITS may allow for the unfair accumulation of individual movement profiles, a "datification" of driving behaviours on which personalized goods and services can be shaped, advertised and sold.

Mobility data may have the same appeal for law and traffic enforcement, beyond the purpose for which C-ITS data are generated and processed. This raises necessity and proportionality concerns on their potential use for these other purposes.

Function-creep is another outstanding data protection risk of C-ITS. The informational asymmetry on the identity of the other peers that is inherent to the chosen broadcast architecture, if not properly addressed with instruments to build trust, might generate

[4] See the examples in the Article 29 Working Party, WP216, Opinion 05/2014 on Anonymisation Techniques.

distortions from the original scope of the communications, diverting users to unintended places. This may happen either due to inaccurate predictions on the state of the environment (e.g. creating a traffic jam rather than reducing traffic load) or even on the basis of a non-neutral interpretation of environmental data (e.g. inducing users to visit specific areas because of economic interests of one of the peers).

4.4 Lawfulness of the processing

It is worth highlighting that Regulation (EU) 2016/679 does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity (art. 2(a)). This exemption may only be valid when strictly limited to the processing that takes place inside a car, and only if the driver is in full control of the processing within the device. It cannot be valid when the device installed in the cars forwards the data of other nearby cars, be it immediately, or as a result of local processing. In such cases the processing is not limited to a strictly personal activity.

Lawfulness for the processing of personal data involved in the functioning of C-ITS must be sought in art. 6(1) of GDPR. Processing shall be lawful only if and to the extent that at least one of the following cases applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Given the scope of C-ITS to improve road safety, foster transport efficiency and promote environmental sustainability, also through the implementation of this European wide interoperable system, the Article 29 Working Party finds that the long term legal basis for this type of processing is the enactment of an EU wide legal instrument (art.6(1)c of the GDPR). It is likely, given the projected prevalence of (semi-)autonomous cars that the inclusion of this technology in vehicles will become mandatory at some point in time, comparable to the legal obligation on car manufacturers to include e-call functionality in all new vehicles. Such a legal obligation should not allow for blanket collection and processing of personal data. The scope of the legal obligation needs to be properly assessed, and validated as proportionate and strictly necessary in a democratic society, as is required under the protection offered by the applicable fundamental rights.

This assessment and law making process should be initiated by the Commission as soon as possible, in order to prevent that the processing of location data and other personal data of EU citizens within C-ITS will take place without a legal basis, and would not be fully covered by an adequate level of protection.

The analysis of the other legal grounds misses some relevant elements. An assessment of the technical capabilities of C-ITS and of its scope may be helpful in this exercise.

Tracking vehicle position, speed and direction is the essence of C-ITS. The higher the frequency of the exchanged messages, the sharper and more detailed the overview of the environment surrounding vehicles, and the better the danger-predicting capability of the system. The Article 29 Working Party understands that the level of adoption and of data contribution is a crucial factor for the operation of C-ITS: poor data contribution, or low resolution of the environmental view captured by each vehicle might affect or even spoil the validity of C-ITS as a tool for road safety.

But triggering adoption does not equal forcing pervasive tracking. The possibility to benefit from C-ITS *per se* should incentivize drivers to adhere freely to C-ITS. If so, a critical mass of users can be reached naturally for a correct operation of the system without any imposition, at the same time leaving people free to select whether they want to participate in the system, and if so, select the tracking options (timing, frequency, locations) that best fit their preferences.

The level of tracking resolution is well represented by the performance indicators of the system[5]:

"A vehicle will generate a CAM approximately every 4 metres and when the driving direction changes with more than 4°. When a distance between current and past position has been changed more than 4 meters or the speed is changed more than 0.5 m/s compared to the last time a CAM is sent but at least once a second and at the most once 0.1 second under normal conditions"

These tracking options are baseline. In fact "*these are the currently defined specifications that may change according to the actual needs of the new functions emerging*", the document states. Also, according to the document, these settings cannot be changed by the user. The C-ITS Working Group thereby strikes a wrong balance between the need to foster the adoption of C-ITS and to prevent 'free riders', that do not participate but enjoy the benefits, by setting the frequency of message exchange (and thus the granularity of the tracking) at the highest possible level.

The C-ITS Working Group has not yet reached consensus on the technical feasibility of obtaining consent. The Working Party underlines that all elements of valid consent have to be met, as outlined in art. 7 of the GDPR and recital 42. Data controllers need to pay careful attention to the modalities of obtaining specific, free and informed consent from different participants, such as car owners or car users. Such consent must be provided separately, for specific purposes, may not be bundled with the contract to buy or lease a new car and the consent must be as easily withdrawn as it is given. Additionally, consent is not an adequate legal ground when it comes to employees, given that the employer-employee relationship is characterized by legal subordination, and employees are not free to deny consent.

In particular, since C-ITS is based on continuous broadcast, there is no point of discontinuity in the transmission to signal intention or wishes on the user's side. Also, broadcasting is an entirely forward-going communication scheme, with no retro-action, and this makes it impossible to set a mutual recognition mechanism between the data subject (sender) and controller (recipient). This lack of mutual recognition by itself should not exclude the use of consent, but makes it more difficult to only process data for specific and well-defined purposes by known data controllers, On the other hand, the assertion made in the document

[5] Processing personal data in the context of C-ITS. Annex I - day one applications, standards & security (A.2.2 CAM).

that consent cannot be considered as a viable legal basis because the controller has not been defined at this stage to a level that would enable the data subject to be aware of its identity is misleading: the existence of well-defined controller(s) is a precondition for the processing itself, and no legal basis under art. 6(1) of GDPR would justify vagueness in its identification. The technical effort to include markers in the structure of CAM and DENM messages to signal users' preferences is a good starting point, but not yet the solution.

The C-ITS Working Group also addresses the possibility of relying on the necessity to fulfil a contract (art. 6(1)b of the GDPR). A specific contract between a data subject and the controller, separate from any other car purchasing/leasing contract, might in principle allow drivers to freely adhere to the system.

On the applicability of the option of joint controllership envisaged in art. 26 of GDPR, it is worth highlighting that this is not a game of strength between the joint controllers, nor is it meant to provide discretion on how to make arrangements in order to partially or wholly skip controllership obligations. The joint controllers that have an established relationship with customers or individuals, and are able to communicate with them directly, should take the full responsibility for informing about the chain of responsibility, the existence and purposes of the other joint controllers.

If processing is necessary for the performance of a specific and freely chosen contract to which the data subject is party, the Article 29 Working Party has repeatedly clarified[6] that this provision must be interpreted strictly and there is a clear connection between assessment of necessity and compliance with the purpose limitation principle. In the context of C-ITS, two aspects are of primary importance. First, it is important to clearly determine beforehand the parties involved in the contract, in order to constraint the processing within the restricted perimeter of the sole actors involved in the scope of C-ITS, and avoid any further use by undetermined other parties. The example provided in the document of a contract between data subjects and a private road operator is incomplete, since there may be other parties involved in the processing (car manufacturers and software developers, for instance) - either acting as joint controllers according to art. 26 of the GDPR, or as a whole in the context of a single consortium bearing the role of full controller - that may establish a contract with data subjects. Second, the rationale of the contract, its substance and goals must precede the processing itself, and controller(s) must test against these rationale and goals whether the data processing is necessary for the performance of the contract with each individual user, taking into account that cars may be driven by owners or other users..

On the possible application of the necessity to process data for a legitimate interest (art. 6(1)f of the GDPR), the Article 29 Working Party recalls that this should not be treated as "a last resort" opportunity for complex cases, where other grounds for lawful processing are difficult to apply. The outcome of a balancing test might determine whether art. 6(1)f of GDPR may be relied upon as a legal basis for the processing. The identification of the controllers and their interests is a precondition, as stated in the document. But other relevant factors should be considered[7]. In particular, the source of legitimacy of the interest (whether it is rooted in the public interest, or in the business interest of a specific party), the impact on data subjects and their privacy expectations, given also the potential sensitive nature of location data, the

[6] Opinion 02/2013 on apps on smart devices, and Opinion 06/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.
[7] Opinion 06/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.

additional safeguards, also from a technical perspective, that could limit any undue impact on them.

4.5 Security

C-ITS is based on the broadcast of messages. Ensuring confidentiality, integrity and availability of communications, i.e. security of communications, in this context needs some extra effort and specifications compared to one-to-one communications.

Broadcast is an unrestricted way to communicate to indefinite receiving parties within the reach of an emitting device. Accordingly, any meaningful way to confine the processing of broadcasted information only to the C-ITS application context, by avoiding that it can be unduly processed by any other non-C-ITS-related receiving party, will rely on the existence of trustable peers and on the consideration that using the data originating from C-ITS for other purposes than road safety would constitute a criminal offence.

It is worth recalling that the legislative proposal COM(2017)10, the e-Privacy Regulation, includes very stringent limitations on the use of "emitted data" like CAM and DENM messages, whereby in art. 8(2) a general prohibition on the use is set forth, except if this is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection, and appropriate technical and organizational measures are in place to ensure a level of security appropriate to the risks, as set out in art. 32 of GDPR.

The document puts a special emphasis on the PKI mechanism as a way to generate trust in the C-ITS system. Actually, PKI is a way to enforce the distribution of a specific information resource (in the case of C-ITS, digital certificates) under a supervised governance structure. PKI does not provide any enforcement mechanism to establish the real intentions of certificate holders or issuers. Unfortunately, collusions or security incidents affecting certification authorities have grown more frequent in the recent past, and there are strong incentives to get certifications only for the purpose of perpetrating malicious actions[8].

The existence of a PKI architecture does not guarantee *per se* the enactment of trust between the peers. Other additional measures are necessary to reinforce trust. The implementation of mechanisms to guarantee security is an important element. Other relevant factors consist in a scrupulous and periodic check on the operations of certification authorities (CAs), either in the form of a cross check between CAs, or by means of audits or inspections carried out by the public institutions involved in the promotion of C-ITS.

Providing integrity means avoiding that data can be altered in an unauthorized way, distorting the proper functioning of an information system. In the broadcast context of C-ITS, this may happen if peers (even trustable peers) manipulate the picture of the surrounding environment by surreptitiously injecting data that are fake, or respond to a business interest rather than to the public goal of road safety. Filtering outliers in the stream of CAM and DENM messages, which might announce out-of-the-average indicators, is a valid deterrence mechanism against malicious use of C-ITS and a way to ensure that the exchanged data are those essential for the purpose.

[8] Edelman, Benjamin. "Adverse Selection in Online 'Trust' Certifications and Search Results." Electronic Commerce Research and Applications 10, no. 1 (January–February 2011).

Availability is the capability of information to serve its purpose when it is needed. This is a very delicate attribute to guarantee in a broadcast environment, due to the presence of a trade-off between time and data quality. If the existence (and thus the availability) of a data related to a potential danger is generated by the concurrent, massive broadcast of messages on that situation, relying on too small a sample of messages might generate many false alarms; on the other hand, waiting until a sufficient amount of evidence is gathered from many different sources might be too late for the safety of people. Preventing accidents is a very crucial result which is expected from the processing of personal data in the context of C-ITS, and the Article 29 Working Party recommends software developers to take the utmost care and make all efforts in designing software programs capable of sorting out false positives and negatives, also by means of collaborative upgrading of the service parameters, in order not to generate alarms or, on the contrary, to undermine the emergence of truly dangerous situations for the data subjects.

5 Required actions

The Article 29 Working Party welcomes the effort made by the European Commission and the Data Protection and Privacy Working Group of the Cooperative Intelligent Transport Systems to incorporate data protection principles in the operation of these new applications since the beginning.

The exercise carried out by the C-ITS WG is a good starting point, but it needs to be complemented with a number of specific actions at different levels. The Article 29 Working Party considers the following aspects of data protection to be particularly relevant:

- The Commission should implement sector-specific Regulations for collecting and processing data in the field of Intelligent Transport Systems;
- The Commission should identify a roadmap for lawful processing of location data of EU citizens in the context of C-ITS applications, where the enactment of an EU-wide legal instrument is the final goal (art 6(1)c of the GDPR);
- The adoption of these legal instruments should start with an assessment of necessity and proportionality of its provisions; moreover, a data protection impact assessment (art. 35(10) of GDPR) should be mandated in the course of the legislative process to clarify risks and mitigating measures from the start;
- The other legal bases envisaged in the C-ITS Working Group Document (namely, consent, performance of a contractor legitimate interest) could be relied upon only if the critical issues identified for each of them in this Opinion can be solved;
- In any of the selected legal bases, the default setting of all installed C-ITS functionality must be switched off.
- The provisions of art. 25 of GDPR (Data protection by design and by default) should be implemented, allowing users to select the tracking options (timing, frequency, locations) that best fit their preferences;
- Security should be reinforced in order to limit the risk of illegitimate use of C-ITS data beyond the scope of legitimate purposes;

- Other privacy by design remedies such as generalization or noise injection should be introduced in order not to affect the overall picture of the environmental status and the possibility to spot a new danger, while limiting unnecessary exposure or long term tracking of the driver;
- Special attention should be given to the frequency with which the certificates are changed, in order to create a fair balance between the selected frequency and the risks of long term tracking.
- Special categories of data and data relating to criminal convictions and offences should not be broadcasted.
- Data quality should be carefully assessed in order to mitigate any risk of non-neutral use of C-ITS, the generation of false alarms or, on the contrary, the misinterpretation of real emergency situations;
- The PKI mechanism for certificate distribution should be publically documented in a detailed way and strictly monitored, in order to limit the risk of collusions between certification authorities and peers, or the intrusion of malicious players;
- The retention periods of the processed data by all the parties involved in the C-ITS platform should be clearly indicated, and it should be prohibited to create a centralised database of the exchanged messages by any of the actors of C-ITS.