# Data Protection and C-ITS - A Use Case

van Haaften, W.F.; van Engers, T.M.; Wennekers, Jennifer

11th ITS European Congress, Glasgow, Scotland, 6-9 June 2016

Paper number ITS-EU-SP0191

# Data Protection and C-ITS - A Use Case

**Wouter van Haaften[1*], Tom van Engers[2], Jennifer Wennekers[3]**

1. Leibniz Centre for Law, University of Amsterdam, The Netherlands, vanhaaften@uva.nl

2. Leibniz Centre for Law, University of Amsterdam, The Netherlands, vanengers@uva.nl

3. University of Amsterdam, The Netherlands

**Abstract**

In 2014 a Cooperative Intelligent Transport Systems (C-ITS) project started in the Netherlands, on the A58 motorway. The project involved an in-car speed recommendation service in order to repulse traffic jams. The project now has become operational in the autumn of 2015. In this paper we will look closer at the legal implications of the project, in particular the data protection issues involved. The data protection issue have become more visible during the building and implementation processes within the project. We will address the data protection issues by looking at the various parts and interfaces within the system and by classifying data streams from a data protection perspective. Moreover, we will spark the development of a data protection framework with which future developments in C-ITS can be dealt with. To this end the A58 Shockwave Traffic Jam System will be mapped on current data protection legislation.

**Keywords:** Cooperative driving, automated driving, data protection

## Introduction

Cooperative Intelligent Transport Systems (C-ITS) are more and more considered to be necessary in combination with self-driving cars. While the self-driving car gets most of the attention of the public, experts in the automotive industry have put their cards on developing a cooperative system; a development European-wide recognized, as can be read from the recent Declaration of Amsterdam[1]. Self-driving cars will become part of such cooperative system as well. Communicating with their environment, other cars and roadside stations, on a permanent basis, they will be able to reduce the safe braking distance required more than by just relying on their own sensors. These smaller braking distances will lead to more available road capacity than will be viable with stand-alone automated vehicles. In the current state of C-ITS, with services delivered to the driver and not directly to the car itself, a variety of techniques can be used to bring the message to the vehicle, such as broadcasting for general messages or cellular or WiFi-p if the message is aimed at a specific driver. Also various types

[1] Cooperation in the field of connected and automated driving (14-15 April 2016).

of messages can be used, mostly specific 'tailor made' advice messages to the driver from a specific service provider. In the latest version ETSI standard messages are being used.
*Cooperative Awareness Messages* (CAMs) provide information of presence, position of the vehicle as well as the basic status of communicating C-ITS stations to neighboring C-ITS stations within a 500-meter range. Also *Decentralized Environmental Notification Messages* (DENMs) are used which are triggered by a cooperative Road Hazard Warning use case or function to provide information about a specific driving related event or a traffic event to other C-ITS stations.

Besides connectivity and standardization issues, all this communication from and to the vehicle and its user, raises questions about data protection. How can 'personal' data be protected and how should personal data be qualified within the C-ITS context in the first place, and how exactly do personal data run through the cooperative system? After addressing privacy issues relating to ITS and the A58 Shockwave traffic jam project last year[2], we now will take a step further by looking into the nature of the data streams involved. Do they contain personal data, and if so how to deal with that? Is it possible to avoid the use of personal data in a cooperative system altogether? In order to get to the answers we will take a look at all the interfaces in one of the C-ITS projects currently run in the Netherlands, the A58 project, in order to find answers to these questions. Before diving into the data streams and interfaces the relevant legal notions on personal data protection will be scrutinized. When is data coming from a vehicle personal data and when isn't it? In legal terms: can a person be identified or is a person identifiable by the data involved? And if so, what will be the legal ground for processing the personal data when the data used by cooperative systems are to be considered personal data, at least in certain cases? Also the position of the controller, as being responsible for the processing of personal data, will have to be looked at in that case. A crucial issue when processing personal data is data security. Without data security there can be no serious data protection. This means that data security within the system will play an important role. But what data should be protected to what extend and at what efforts? And how will be assured that all stakeholders will comply with the legal provisions that will be applicable to cooperative driving? Next to these legal provisions and the data streams within the A58 project this paper also is an attempt to provide new perspectives that can be scrutinized while preparing for the implementation of C-ITS services.
In order to being able to control the relation between the technical developments and the data protection requirements a data protection framework should be developed. The analysis in this paper could be the basis for such framework that could function as a preliminary privacy impact assessment on the one hand and as a 'privacy by design' manual on the other hand.

**The Shockwave Traffic Jam A58 Project**

The A58 project provides drivers on the A58 motorway with speed advice in order to get a more

[2] ITS nr 2665-2015 van Haaften, van Engers Data protection and cooperative driving

regular traffic flow and thus to avoid traffic jams due to driver behaviour on busy roads. The A58 project comprises a chain of processes involving different parties. The functional decomposition (fig 1.) shows the project environment and the players involved.

The A58 project is not the only project running with cooperative technology. Also the Corridor project between Rotterdam and Vienna uses similar data and transmission technology. However, at this moment the A58 project seems to be in a phase where most technical choices are stabile and the data sets as well as the interfaces have been defined and are actually being used.

The business model for the SP's lies in the supply of a speed recommendation to the customer on the A58. Along with this information other location bound information - like special offers by roadside filling stations or other shops in the neighborhood - can be presented to the driver. Both the user and the suppliers of special offers and information are potential customers for the SP. For this service a minimum of information from the user will be required, depending on the business model of the SP. In one of the models, for instance, only the companies that offered products to the drivers on the A58 are paying the SP. In that case the users, whom were given an on board unit could remain close to anonymous. Only the fact that 'someone' is driving on the A58 is relevant at that particular moment, both for the speed recommendation as for the presentation of the special offers from the sponsoring companies. Who is driving the car is not relevant for the delivery of the speed recommendation service.

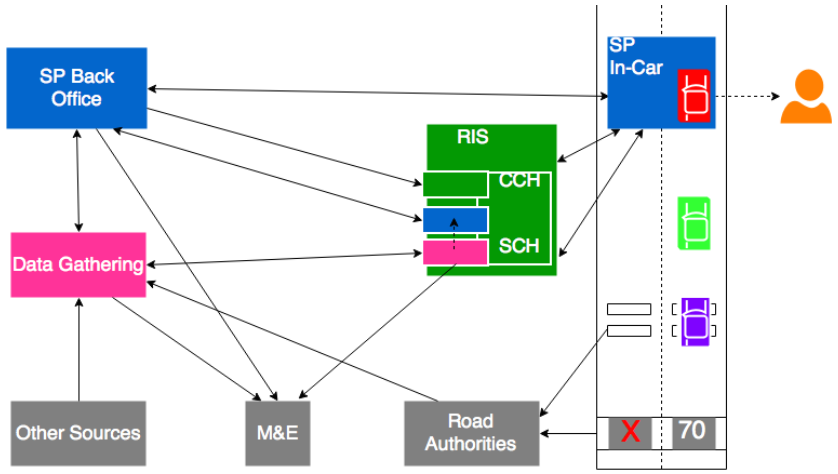


**Figure 1 - Functional decomposition of A58 project (CCH=Connected Channel, SCH=Service Chanel)**

The SP's in the A58 project collect their data by acquiring on-going traffic data from the user's vehicle. This information is enriched with data from other service providers by the SP or by running the data from the vehicle through the data providers' system. Eventually the SP will use all data available for the relevant section of the highway for the production of the recommendation. That recommendation will be sent via the roadside service provider to the driver within seconds. The system therefor requires

technical components such as an on-board-unit (or smartphone) in the car and a telecom platform. Looking at the architecture of the A58 project the question is what data the interfaces will be processing and what personal data will be amongst these data.

**Privacy by design**

Within the development of C-ITS, data protection will play an important role. In order to anchor that role within the development process the data protection framework should be structured in such a way that in any stage of development a reflection on the data protection issues will be facilitated. While using the framework developers should be able to design C-ITS applications that either can function without personal data, or that can deal with personal data in a law compliant way.

The emphasis within such a framework will be on the technical and organizational parts of the application that actually deal with information from the vehicle, and thus possibly from its owner/driver. In cooperation with the suppliers of C-ITS components and with C-ITS service providers a set of criteria should be developed that will allow these parties to make balanced choices as to data protection issues. They could for instance choose to change their service in a way that personal data will no longer be required. Or, if personal data are inevitable, they could build in informed consent in a way that will lead to a minimal disturbance of the service for the user.

The data protection framework should help developers to gain awareness on the topic of data protection and to integrate data protection into their development skills. The framework will not be a classic privacy impact assessment because it will have its affect before an assessable product or service has been built. A well designed C-ITS service or product developed according to the privacy by design standards laid down in the data protection framework should have no problem passing the privacy impact assessment when it is being implemented.

The data protection framework serves as evaluative framework as well as it sets some important design requirements well in advance when developing new services. The framework should therefore be precise enough to allow systems designers to test their designs. The input of legal experts willing to take ‘a stance in advance’ is necessary in order to decide on specific consequences of the quite open norms described in the European Data Protection Directive. Unfortunately many legal experts prefer to wait for court decisions to clarify things, a position which is not helpful to the systems designers and the organizations they represent, as C-ITS will demand substantial investments, investments that will only be made if the investors can trust that their solutions meet legal demands.

In order to be able to design such data framework different conceptual frameworks have to be mapped. The car manufacturing, telecom industry, IT and Law use different terms and concepts and without proper mapping between the ontologies relevant to these domains one cannot expect that experts with different backgrounds can understand each other. Since developing ontologies and ontology mapping are rather IT technical matters that don’t fit the rest of this paper’s content we won’t elaborate on this topic here but address this in another publication.

**Compliance and enforcement**

Also the question of compliance and enforcement of data protection law will have to be addressed. Regarding the vital interest of safe and reliable cooperative systems, a solid legal basis will have to be backed up by serious enforcement. In this way compliance with the data protection rules all over the EU can be maintained. One of the issues with the application of legal notions in cooperative driving is that in such a multi stakeholder environment, multiple interpretations of those legal notions can be adopted. This not only means that the regulations will have to be crystal clear[3], but also that the application of the regulations within the cooperative system should be monitored on a permanent basis. The risk of misuse of protected data will grow with the number of applications where C-ITS has been implemented. Surveillance of the application of the standard will be necessary in order to be able to guarantee a secure and compliant operation. A non-intrusive compliance monitoring system could eventually be the way to make sure that data protection laws are being obeyed. Using such a system, that should be part of the (privacy) design, we can also guarantee that technical and communication standards that will have to preserve the security of the communication and thereby the safety of cooperative driving system will be safeguarded.
In this perspective we are now taking a first step: a man-controlled cooperative driving service and the data protection aspects thereof.

**Data protection implementation**

How will the transformation of a very private activity like driving a private vehicle oneself into a 'cooperative inactivity', being driven by the cooperative automated vehicle, relate to our legal framework of data protection? How can our privacy be protected in a vehicle that is in constant communication with the environment? Would you, being a car driver, still want to be part of that data explosion, or would you rather be an anonymous passenger that cannot be linked at all to the car data, driving data like location, speed and direction? In-car privacy can be classified as a subjective right and as a personality right. This implies that the grantee has an exclusive claim against the others, the government included, while the others have a corresponding duty towards him (Hohfeld 1920) to respect the privacy of the subject. How to deal with this claim and corresponding duty within the framework of cooperative driving will be one of the major challenges for the years to come.
One of the best ways to avoid infringing the privacy is not to process personal data at all. In that case data will be processed anonymously. When the data are being anonymized the personal data of the subject(s) in the car will be not be attached nor will be attachable to the user data of the vehicle. If this status can be fully achieved, then the data from the vehicle will no longer classify as personal data. Data protection law will then no longer be applicable, personal data rights will be respected entirely.
Although this solution seems very attractive, practice shows that anonymity of data sent by a vehicle to a service provider will hardly ever be really anonymous. Eventually the data will be traceable to the

3 Hopefully the new Data protection regulation is going to help on this aspect.

data of the vehicle *(Vehicle Identification Number[4])* and the data of the owner, or the data of the participant of the cooperative service. But it remains a situation worth striving for from a data protection perspective. However, if the C-ITS data from a vehicle are to be considered personal data, then these data can only be processed with a legitimate legal ground. So what are personal data in this context?

**Personal data**

Personal data have been defined in the Directive (EG) nr. 95/46, Article 2a as; 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

In the A58 project the information sent by the participating vehicle via its on board unit will contain an identifier that will link the on board unit to the system. That raises the question if personal data is being processed or not. The key question is: can the information from the on board unit eventually be matched with the customer of the service in a way that reveals his or her identity? This customer often is the owner of the car or at least a regular user of the (e.g. leased) vehicle, due to the character of the service aiming at regular users. But also situations are possible where the link between the on board unit information and the actual user of the car will be less obvious. Although this issue will not be scrutinized within the framework of this paper, a brief inventory of possible relations within the A58 project will be made.

Suppose the case that a private car owner participates in the A58 project and drives the car himself. His in-car device sends the information conditional to the C-ITS service to the roadside. Will this information be personal data by nature, or will that depend on the content of the message sent? In other words: will the owner be identifiable from the signal that is sent to the roadside even if the message only contains in itself unidentifiable information? Or to turn the question around: will it be possible to run a C-ITS project like the A58 without processing personal data? The following situations may illustrate the possibilities when information is running from the in-car system to the A58 system:

1. Vehicle owner = participant C-ITS = driver
2. Vehicle owner = participant C-ITS ≠ driver
3. Vehicle owner ≠ participant C-ITS = driver
4. Vehicle owner ≠ participant C-ITS ≠ driver

In these examples all entities are supposed to be natural persons. In the first example the car user owns

4 In January 2016 the German Privacy Commissioners along with the German car industry have agreed that data in the vehicle will only be regarded as personal data if itcan be linked to the vehicle identification number or the licence plate number.

the vehicle, is also participating in the cooperative system and drives the car himself. All three conditions coincide, probably the most common situation. In the second example the vehicle owner, is also participating in the cooperative system, but is not driving the car himself. In the third example the driver is the participant and although he is not directly coupled to the vehicle registration, he is still registered in some way at the service provider. More indirectly related are the owner and the driver in the fourth example. Here for instance the owner of the car could be the lessor, the user could be the employer and the driver the employee. Although in all cases personal data may be involved, participating in the service does not always reveal the same amount of personal data. In the A58 project for instance, participation does not require the submission of more personal information than an email address, a nickname and an on board unit ID. The SP will receive a dataset containing the identification of the on board unit and the location and speed of the vehicle. That is all the information necessary to provide the speed recommendation service. The question to answer in all foursituations is: to what extend will either one of the car related parties be identifiable from that information? In all examples the *participant* will at least be traceable back to his email address and nickname. This address is in itself traceable to the ISP providing the email service. So if the participant is the same person as the driver, the one that generates the location, direction and speed information, then this driver could be identifiable. However, when the participant is the owner, and the driver has a more distant relation to that owner, then the driver will be less identifiable. When all three roles are with different persons' identification of the driver could even be more difficult. For the moment it seems that the identification of the driver is the reason to consider the data sent from the vehicle to the roadside system personal data that requires a legal ground.

**Data protection legal grounds**

To be able to process personal data a legal basis for processing those data will be necessary. Various legal bases as given in Art. 7 of the Directive could be applicable in this case.

a) The most obvious one, now used within the A58 project, is 'informed consent'. With the explicit permission of the data subject a lot of processing can be done as long as legal standards are being maintained.

However, this ground will lead to a vast amount of administrative handling and will therefor not be very comfortable to use. In terms of Hohfelds classification the participant will grant the right to infringe the participants' privacy, to the SP and will have the liability to tolerate this infringement until further notice.

b) Less obvious but worth looking at is the processing necessary for the performance of a contract between the data subject and the controller, in this case the contracting SP. This will reduce the administrative handling, but is less strong a consent as the informed consent of Art. 7.a. As it comes to the legal classification in this case the legal relationship has already been established with the service provision agreement. The service provider has an obligation (duty) to deliver the service and the customer has a right to that service. In order to perform its duty, the service provider will need to process the personal data of the customer. The question is whether this contract provides an

autonomous right to process the personal data and whether the customer has the duty to accept the processing of his personal data merely on the basis of the service provision agreement.

c) Compliance with a legal obligation is not a ground for processing personal data within the A58 project since no such legal obligation exists. However, that could be different when C-ITS services will directly be connected to the in-car management systems for steering, accelerating and decelerating. It seems logical that, in that stage of C-ITS application, legislation will be the basis for self-driving cars combined with C-ITS technology. The establishment of legislation that will force the road user to share his personal data means, in terms of legal classification, that the service provider is empowered (power) to process personal data for this particular application. On the other hand, the car driver will be disabled (disability) to oppose to such an infringement of the protection of his personal data.

d) In the current interpretation the protection of vital interests of the data subject will not easily qualify as a legal ground for the processing of personal data. Without a service provision agreement between the data subject and the controller, the data subject has no interest at all, let alone a vital one. And when a service provision agreement has been established the legal ground under b) seems to be more appropriate. One imaginable situation where this ground could be valid is when the only way to drive safely is within the cooperative system and the law does not provide for an obligation to join the system as under ground c). In that case the service provider could claim the right to process the personal data and the customer would have no right to oppose.

e) This legal ground is reserved for public interest, and therefor not obvious as a legal basis in this phase of cooperative driving. However, when cooperative driving evolves in combination with automated driving this could well be the legal basis when pursuing road safety. The public interest would require legislation implementing the exception foreseen in the Directive. In this legislation a power would have to be created for the authorities and the parties running the system to use the data from the vehicle within the system context. This would lead to another legal ground, c), for the processing of personal data. On the other hand, a disability would have to be created for the user(s) of the vehicle to exercise their privacy rights, despite their fundamental character. The road user will be granted the right to participate in a safe cooperative driving system. The cooperative driving authority will have the duty to provide that system. Eventually this could deliver an acceptable solution provided that the personal data involved can be properly secured.

f) Also worth looking at seems to be this ground covering the processing that is necessary for the purposes of the legitimate interests pursued by the controller. Regarding this ground the EU privacy Commissioners[5] have prescribed the way in which this ground could be applied. Whether processing is necessary for the purposes of the legitimate interests pursued by the controller should be balanced against the interests of fundamental rights and freedoms of the data subject. Developing this balancing test specifically for C-ITS applications like in the A58 project could be taken into consideration, thus

[5] Art 29 working group , Opinion 06/2014, 844/14/EN WP 217

creating an easy to use, predictable and balanced legal ground for C-ITS. In terms of Hohfeld's classification the service provider would have a right to process the personal data and the customer would have the duty to accept this processing under the conditions referred to in the balancing test.
All suggestions made here will be subject to further research within the framework of the Dutch C-ITS program.

**Shockwave Traffic Jam System**

Being able to communicate between vehicles and service providers and between vehicles and other vehicles is essential for cooperative driving. Different communication (network) protocols and communication standards have been developed over the past decades. Within the project developers have focused on two specific network protocols; cellular or LTE networks (2.5G-4G) that are similar to the ones we use for mobile devices such as smartphones, and the IEEE 802.11 Wireless Local Area Network Protocol (WLAN). Within the A58-project these different network protocols are the indicated as respectively *connected* and *cooperative* ITS, although no clear functional distinction between these protocols exists. Performance issues, i.e. bandwidth and speed, availability, operational structures and costs etc. however vary between them, which may make one more appropriate given some use context than the other.
Both these technologies enable vehicles to communicate with each other or with devices on the roadside, so that data can be exchanged between car and provider, and vice versa[6]. The data gathered can be used for collision avoidance, incident management, navigation, vehicle identification and location, etc. Within the A58 project it is only being used for in-car speed recommendation.
In the next paragraph we aim to explain the two distinguished communication technologies, connected (3G and 4G) and cooperative (802.11 p), in more detail, as some of these details have consequences for the data exchange, the parties involved and the legal framework that defines, data ownership, protection, access and use rights.

**Communicating vehicles**

In figure 2 the architecture of the A58-project is sketched. From the figure we can read that the vehicle is conceptualized as some vehicle infrastructure (VIS) that allows for applications that can run on top of this infrastructure. Details about the different layers of this VIS are left out as the focus of this paper is on the two different communication technologies that can be used between vehicles and service providers. The typical difference between the two distinct communication technologies is that the technology indicated as *connected* is based upon cellular network technology that is commonly used for mobile communication for which many telecommunication services providers already have set up networks that are also very well interconnected. For the technology indicated as *cooperative* that is

6 Spookfiles A58 - OCD en Solution Design - Het gemeenschappelijke eindrapport (deliverable) van de Haalbaarheidsfase WP1 in het Spookfiles A58 Project, 2014

based upon WLAN technologies, such interconnected networks still have to be created. One of the problems for inter-vehicle communication is the required data-exchange speed, which with currently available networks cannot always be guaranteed. The cooperative technologies at this moment offer a much higher data-exchange speed, but since these technologies are only suited for short-range communication while the connective technologies are suited for long-range communication they will require a vast roadside infrastructure.
The current limitations in bandwidth and communication speed put constraints on the possible technical data-protection measures one could take as part of a secure solution. Complete public-private key encryption of data before sending it to the receiver and consequent de-encryption at the side of the receiver before processing it, would further slow down communication speed and consume more bandwidth. For this reason the developers of cooperative driving infrastructures have decided to only consider a quite limited form of data encryption including a Public Key Infrastructure (PKI)[7], thus requiring less of the communication technology, but introducing more risks with respect to possible data infringements.

Communication for connected ITS is based on infrastructure-based communication technologies, such as cellular networks (3G, 4G, GPRS, etc.), WiMAX, DVB, etc. Referring to the architecture in 2, the vehicle will exchange data directly with the Service Provider, without any interference of other parties. In the first 'connected' phase of the project cellular networks were used, specifically the 3G and 4G (third and fourth generation) standards, as these connected technologies are most used within the applicable area of the project, the Netherlands. Within the EU Platform on C-ITS (Working Party 5) definitions have been developed on both connected and cooperative C-ITS[8].

---

7 Public Key Infrastructure = a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption to facilitate the secure electronic transfer of information within the C-ITS system.

8 In WP5 of the EU Platform on C-ITS both connected and cooperative C-ITS have been defined:
The definition of cooperative is the following:
' Cooperative means that the data will be sent from roadside to and from the vehicles (V2I2V) and between vehicles (V2V) [by all communication means but mainly] by short/range WiFi-p (control and warnings) [and less by cellular 3/4G/LTE (for less critical services)]. In the "cooperative" situation real coordination takes place between vehicles mutually and between vehicles and roadside. This coordination can take place by a driver action (max speed; initially during day one) or automatically by the vehicle systems themselves (eg CACC)'.

Within the A58 project based on the EU definitions the first 'connected' version is the cellular version and the ultimate 'cooperative' version will be based on the WiFi-p protocol. As is shown in fig 1. connected ITS implies a (cellular) connection between the in-car service and the back office of the telecom service provider (3G and 4G) via a (roadside) telephone tower. However, this technology cannot provide the speed and bandwidth required for fast car to roadside and car to car communication. Therefor the project will use

**Interfaces in the A58 Project**

What data protection issues arise at which A58 project interfaces? To be able to get a good picture of the personal data passing each interface in the system the interfaces will be scrutinized one by one, or grouped where appropriate and possible.

The following interfaces can be identified:

A- From Back office data collection to SP Back office
A*- From road side data applications to roadside SP applications
B- To and from SP Back office and in-car applications (connected)
D1- From SP Back-office to Road side facilities
D2- To and from SP application and SP Back office
D3- From Road side system to in-car application
D5- From in-car application to roadside
D10- To and from SP applications and Road side facilities
D11- From SP and Road side facilities to Road side network and transport
F- From roadside facilities to road side data applications (=D10),
F*- To and from Road side data applications and Back office data collection
G- From SP back office to Back office data collection
H- From Road Authority traffic management center to back office data collection
H'- From SP Back office to Road Authority traffic management center
H*- From Road Authority road side system to road side data application
I- To and from the user to the in-car applications

the ETSI standardised Wifi connection (802.11 P) between the in-car service and the roadside system, established for its low latency and short range communication.

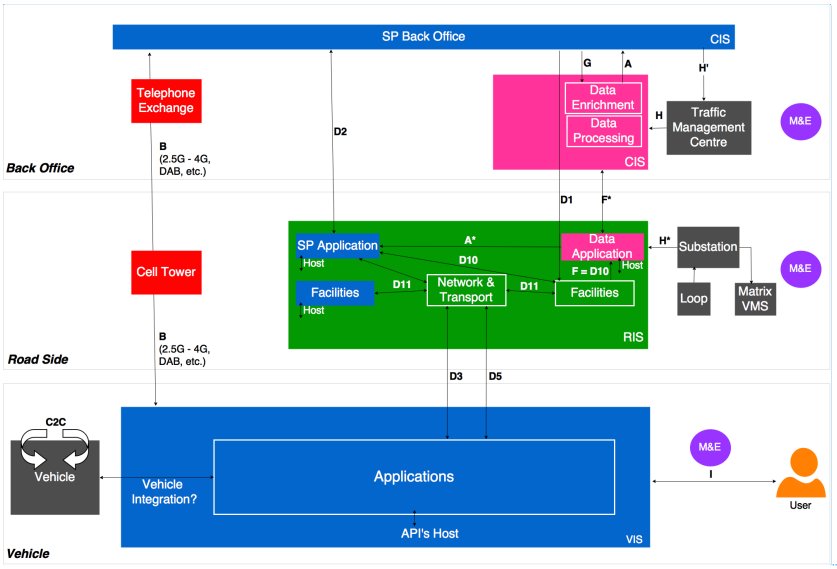


**Figure 2 - Architecture A58 Project**[9]

**Met opmerkingen [JW1]:** D3: Moet een pijl naar beneden zijn

D5: Moet een pijl omhoog zijn.

Beiden moeten uni-directional zijn

The architecture consists of four different parts:

1. The Back Office, with the Central ITS Station (CIS);
2. The Road Side, with the Roadside ITS Station (RIS);
3. The Vehicle, with the Vehicle ITS Station (VIS);
4. Cellular communication network.

1. Within the limited scope of this paper two groups of similar interfaces can be distinguished. Data collection and exchanging between Service Provider and in-car applications (interfaces A, A*, D10, F, F*, G)
2. Data exchange with the road authority (H, H', H*)

When a legal ground has been found, data traffic within the system passing all the interfaces involved can start. Working outside in and inside out the interfaces will be looked at in their sequential order in the SP process. Therefor we will start with the interfaces involving the driver or the car, then work towards the SP back office, and back again.

9 Unlike in the figure D3 is for data transfer from the roadside to the car and D5 is for data transfer from the car to the roadside.

*B - To and from SP Back Office and In-Car Applications*

This interface has been used in the first phase of the A58 project, the connected phase. In this phase the in-car device, a smart phone, was more or less directly connected to the back office of the SP. The data set surely contained personal data, the smart phone of the participant was registered as a mobile phone with all the personal data consequences thereof, and the SP added identifiable data as well as location data. In principle the end-to-end connection with the smart phone is well protected. It is an often used proven interface that delivers the information to the SP via the telecom provider. Potential data protection leaks are to be looked for in the back office of the SP and its partners, not as much in the cellular connection. So why not go connected then? One of the problems with the connected version of the service is latency. The message could be underway for as much as minutes and that could be too long for an application with road safety implications. That will be even more difficult once the messages will be delivered directly to the in-car management system of a self-driving vehicle. In that case steering and breaking will depend on the system, which means that the latency should be next to none. As far as the confidentiality was concerned: the data ran from the telecom provider straight into the SP back-office.

*D5- From in-car application to roadside*

This cooperative interface between the car and the roadside system is the first step from the data subject into the cooperative system. The interface has been foreseen as supported by WiFi-p. This technology enables very low latency between car and roadside, suitable for self-driving applications. However, in order to gain from this low latency no encryption should be applied on the messages from the on board unit or other devices. The lacking of encryption means that anyone can receive and read the signal of the car within WiFi-p range. The messages sent from the car to the roadside station may not be encrypted; they are protected by a public key infrastructure (PKI). This PKI authenticates the messages, to make clear that it has come from a legitimate participant. The PKI process itself has all kinds of security rules that have to be followed, regardless the content of the message, and its possible personal character. All roadside stations and participating vehicles will have to be part of the A58 security system.

*D11- From the roadside to the roadside service provider facilities and back*

This interface brings the messages that are collected directly coming from the vehicle to the RIS facilities. It is merely transportation of the data coming in via interface D5. However, it could contain personal data which will be accessible to the road side service provider, so the appropriate care will be necessary.

*1 - To and from the various services engaged by the leading service provider*

In this interface the processed data is being sent and processed by and between the service providers that have been engaged to do so by the C-ITS service provider/controller. Whether these data contain personal data depends on the information model of the SP, in particular if personal data remain part of the dataset once it has been received from the users vehicle. If not, then these interfaces will not have

to deal with personal data. If so, however, the SP will have to make sure that all parties engaged in the processing of the personal data are aware of that fact and have been instructed to obey the legal terms for the processing of personal data. This is merely an organizational matter. The controlling SP will have to make sure that all legal provisions related to the processing of personal data will be respected.
The A- and A*-interfaces serve to collect data related to traffic flows and independently moving vehicles. The collected data is sent from the Back Office data service providers to the SP Back Office, and from the roadside data application to the SP's applications. Whether these data contain personal data depends on the information model of the SP, in particular whether personal data remain part of the dataset once it has been received from the users' vehicle. If not than this interface will not have to deal with personal data.
The D10 interface exchanges information between the RIS facilities and the SP applications. It could well be processing personal data and appropriate measures will have to be taken in order to make sure that the data is not misused. The F- and F*-interfaces collect Cooperative Awareness Message (CAM) and Decentralized Environmental Notification Message (DENM) based information, regarding incidents and warnings, and exchange it between RIS facilities and the RIS data application, and the RIS data applications and the Back Office. In the A58-project, this information would be passed on via the A- and A*-interfaces to the SP's applications and back-office.
The G-interface is used for the enrichment of the data received from the car and other sources. Currently, many SP's use 'Floating Car Data', which is sent through mobile cellular networks to customers – therefore through 'connected' technology. However, in the A58-project, this type of data could be used, and could therefore be delivered through the G-interface to data-gathering parties in order to improve the data quality.

*2 - To and from the Traffic Management Center*
Interfaces H, H' and H* are the interfaces that are connected to the road authority, specifically to the Traffic Management Centre. Through these interfaces, gathered data (in raw, enriched or otherwise processed through the CIS) is offered to the Off Board functionality, and feedback can be returned to the Traffic Management Center. No personal data will be passing these interfaces since the most of the data will be anonymized floating car data.

*D1: Exclusive unidirectional channel SP - RIS*
Interface D1 offers the leading SP a transparent communication channel from its back office to its own Vehicle ITS Station (VIS), through the roadside substations. D1 is a unidirectional channel from CIS to RIS. It can be seen as a connection between the software of the SP, and the application in the RIS (Roadside ITS Station). In the RIS area, coding and broadcasting of the offered information is timely performed, to every VIS within reach. When personal data will be sent the SP will have to make sure that the entire line from back office to the vehicle is well protected and all legal obligations are met.

*I: User interface*

The I-interface serves in the A58-project as a connection between the user and front end on-board-unit, which has a cooperative module added.

*D2*

The D2-interface links all communication from RIS to CIS and vice versa. It is entirely within the domain of the SP. Possible processing of personal data shall have to be dealt with within the SP's organization.

*D3 - From the roadside to the in-car application*

The D3-interface links all communication from RIS to VIS. Offers support for ITS G5 (802.11p) messages, but also allows Service Providers to send from CIS and RIS Service Provider-specific information to their own VIS. Whether it contains personal information depends on the information model of the SP. In order to get the message with its customer a broadcast with a PKI security and authentication facility could probably be delivered in the car without containing personal data. If the message contains personal data however than all legal and security requirements will be applicable. This is particularly important because, in order to gain from this low latency, no encryption must be applied on the messages to the on board unit or other devices. The lacking of encryption on the message itself means that anyone can receive and read the signal to the car within 802.11p range.

**Conclusions**

In this paper we have addressed a number of issues concerning data protection in C-ITS. The question how data protection can be guaranteed has no easy answers. For a successful implementation of C-ITS it is essential to look into some legal notions. It is crucial to determine if data coming from the vehicle always qualify as personal data, and if so what the grounds for the processing of those personal data are. We also have to find a way to organize data security when the vehicle will send out unencrypted messages with its WLAN. To get answers that will enable the development of C-ITS a new match will have to be made between current legislation and jurisprudence on data protection on the one hand and the technical developments in C-ITS on the other hand. This requires collaboration between two quite different disciplines and professional practices, law and IT engineering. It has to be stated here that the conceptual mapping between these different domains can never be a static one. The norms on data protection and privacy are deliberately been defined in quite broad and open terms, this way ensuring that these norms may last a while. The technologies that are developed in ICT supporting C-ITS on the other hand are rapidly developing and so are the business models of the service providers. Alignment of the conceptualizations from these different domains is necessary and should precede the developing of C-ITS practices. The outcome of this ongoing process should be the basis for putting into practice Privacy by Design. This practice should contain well-engineered technology and processes but should also include standards for organizing the stream of data in the various back offices involved. This will

call for a closer cooperation between the legal and the data management sides within C-ITS. Only that cooperation can provide us with legally sound software. The modeling approach developed by the Leibniz Center for Law in collaboration with others based on the Hohfeldian breakdown of legal notions (see Van Engers & Van Doesburg 2015) can help us to develop transparent and accountable services that can be monitored at software/system level without intrusion in the data processing itself. All these elements will have to be part of the Privacy by Design to prevent data protection becoming a showstopper for C-ITS.

**References**

1. T. van Engers & R. van Doesburg (2015). At your service, on the definition of services from sources of law. In *Proceedings of the 15th International Conference on Artificial Intelligence and Law* (pp. 221-225). New York: ACM
2. W. van Haaften & T. van Engers (2015) Data Protection And Cooperative Driving.In *Proceedings of the 22nd World ITS Conference* (ITS-2665), Bordeaux.
3. Hohfeld Fundamental legal conceptions as applied in legal reasoning, 1920, Edited by Walter Wheeler Cook 2010,
4. Directive (EG) nr. 95/46 on data Protection, 24 October 1995