Conférence Européenne
des Directeurs des Routes

Conference of European
Directors of Roads

ANACONDA

Report on Implementation Road Map

Deliverable No 6.1

17 July 2017

Project Nr. 850708

Project acronym: ANACONDA

Project title:

Assessment of user Needs for Adapting COBRA including ONline DAtabase

Deliverable No 6.1 – Report on Implementation Implementation Road Map

Revised date of deliverable: 30.04.2017

Actual submission date: 26.04.2017

Resubmission with revisions: 17.07.2017

Start date of project: 01.09.2015 End date of project: 31.05.2017

Authors of this deliverable:

Kerry Malone, Somayeh Djafari (TNO, the Netherlands)

Version: 1.0 (17/07/2017)

Disclaimer

This work has been supported by data contributions from national road authorities. The information and views set out in this report are those of the author(s) and do not necessarily reflect the official opinion of the national road authorities. Neither the national road authorities nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

Revision and History Chart

Version	Date	Comment
0.1	2017.03.15	KM: create initial document structure, initial text
0.2	2017.03.18	SD: added legal text
0.3	2017.04.04	KM: modification of chapter 2, addition of roadmap elements
0.4	2017.04.07	SD: modification of chapter 3, addition of legal text
0.5	2017.04.12	KM: additions to Executive Summary and Conclusions
0.6	2017.04.20	Reviews of Document
0.7	2017.04.25	KM: revisions based on reviews
0.8	2017.04.26	KM: final revisions
0.9	2017.06.21	SD: feedback ASFINAG; KM: revision based on PEB feedback
0.99	2017.07.13	KM: additional revisions
1.0	2017.07.17	MA: formatting of report

Executive summary

The "Assessment of user needs for adapting COBRA including online database" (ANACONDA) project builds on the COBRA (COoperative Benefits for Road Authorities) project. That project developed the spreadsheet-based COBRA tool for National Road Authorities (NRAs) to use to examine the business case for deployment of Cooperative Intelligent Transport Systems (C-ITS) on their roads, using evidence gained in an investigation of impacts and deployment issues. The COBRA+ tool builds on the strengths of the original COBRA tool. The new COBRA+ tool was enhanced with new functionalities, greater geographic coverage and more flexibility, to enable NRAs to compare the costs and monetised benefits of C-ITS in various contexts to support investment decisions under different deployment scenarios.

The COBRA+ Tool supports decision-making for the short and medium term (2-7 years), while calculating the impacts to 2030. The short and medium term includes the possibility to deploy cellular 3G/4G and ITS G5 communication platforms, where the ITS G5 in-vehicle units are hybrid, enabling 3G/4G and ITS G5 communication. The short and medium term excludes 5G cellular, due to the uncertainty in the required developments and subsequent standardisation required for the mobility applications. The Tool allows the choice of a wide range of other parameters, from services to be deployed to equipment rates of vehicles and infrastructure. Deliverable 3.2 [Ognissanto et. al., 2017] provides an overview of the parameter choices.

This deliverable identifies key actions in the short and medium term (2-7 years) for Road Authorities as they prepare for the deployment of C-ITS. These key actions are based firstly on the findings of the three use cases investigated in the ANACONDA project. They take into account the choices that National Road Authorities face in terms of investment (communication platform, the level of equipment, deployment period, whether to implement infrastructure savings), the services to deploy, the choice of business model, and the results of these choices in terms of impact on safety, efficiency and environment, the benefit-cost ratio and the costs and benefits that the National Road Authorities incur.

Secondly, this deliverable identifies the legal enablers and hurdles for the deployment of the services investigated in the ANACONDA project. The analysis focuses on the areas of privacy, liability and data access, considered to be the most important issues to handle within the budget and timeframe of ANACONDA.

National Road Authorities need to take several actions to prepare for the roll-out of C-ITS in the areas investigated in the coming 2-7 years.

- In the area of liability: when engaging in new business models based on traffic data, specify the quality of the data and services provided in detail and carefully define contractual obligations combined with a set of buyer's duties to verify the data received prior to its use in order to reasonably limit liability.
- Privacy brings a number of new requirements for National Road Authorities and other parties involved in the chain of C-ITS delivery, requiring action before and after the General Data Protection Regulation (GDPR)(2016/679/EC) enters into force on 25 May 2018. In addition to contributing to ongoing discussions addressing privacy and data protection with other stakeholders, these include carrying out a privacy impact assessment, examining privacy-enhacing technologies, developing transparency toolds, developing empowerment tools and establishing privacy governance.
- Establish measures to ensure access to data within own organisations. For access to other data, they should take part in on-going discussions with other stakeholders at the European and national levels.

- Investigate the many parameters in scenarios using the COBRA+ Tool, to prepare for the decisions to be made and to identify areas for deeper analysis using more detailed information or models.
- Work to realise sustainable business models.
- Actively follow or participate in 5G technical, standardisation and security developments to support decisions on whether and how to integrate 5G into future C-ITS deployment.

Table of contents

List of tables

List of figures

1 Introduction

1.1 Background

The trans-national research programme “Call 2014: Mobility and ITS” was launched by the Conference of European Directors of Roads (CEDR). CEDR is an organisation which brings together the road directors of European countries. The aim of CEDR is to contribute to the development of road engineering as part of an integrated transport system under the social, economic and environmental aspects of sustainability and to promote co-operation between the National Road Administrations (NRAs). The Mobility and ITS call has three sub-themes, one of which is “The business case for connected and co-operative vehicles”. The ANACONDA project falls into this theme.

Cooperative systems communicate and share information dynamically between vehicles or between vehicles and the infrastructure. In so doing, cooperative systems can give advice or take actions with the objective of improving safety, sustainability, efficiency and comfort to a greater extent than stand-alone systems, thus contributing to road operators’ objectives.

The ANACONDA project builds on the COBRA (COoperative Benefits for Road Authorities) project. That project developed the spreadsheet-based COBRA tool for NRAs to use to examine the business case for deployment of Cooperative Intelligent Transport Systems (C-ITS) on their roads, using evidence gained in an investigation of impacts and deployment issues. The ANACONDA consortium has continued this support to NRAs by:

- Extending the number of countries, functionality and C-ITS covered by the original COBRA tool
- Assisting CEDR countries in the preparation and use of the updated tool, COBRA+
- Developing the COBRA+ Monitor, an online tool for the monitoring of C-ITS implementations by CEDR members
- Developing a roadmap for transition to C-ITS-equipped motorways.

This deliverable identifies key actions in the short and medium term (2-7 years) for Road Authorities as they prepare for the deployment of C-ITS. These key actions are based on two pillars. Firstly, the actions are based on the findings of the three use cases investigated in the ANACONDA project. The use case analyses in the COBRA+ Tool provided insight into the key parameters that affect the Benefit-Cost analyses and business cases of the Road Authorities. Issues such as spectrum allocation, standardisation of input beyond day-one services and processes such as compliance assessment are not addressed in this analysis. Secondly, the actions to address legal enablers and hurdles in order to deploy the ANACONDA services in the areas of privacy, liability and access to data are identified. Finally, these actions are combined into a roadmap.

Legal issues in the area of C-ITS are being discussed at the time that this report is being produced. Simplifying the process greatly, there are two major steps with respect to realising measures that comply with relevant law. Firstly, one must create a framework in which the issue at hand is dealt with. Secondly, this framework needs to be checked for compliance with relevant law. At this moment, Data protection and privacy, and access to data, are in the first step: the frameworks are in development. This means that once the formulation is ready, they need to be checked for compliance.

Active discussions in Europe are taking place in the area of privacy and data protection and access to data among a wide variety of actors. Reporting on these in this report in detail is outside the scope of this project. The outcomes of these discussions are not yet known; there is even disagreement among key groups of actors in some instances. When agreement is achieved, these agreements need to undergo assessment to determine if they comply with the law. Road Authorities should actively take part in these processes and discussions. Until the time that the results are available, no definitive conclusions can be drawn about the outcomes. Road Automrities should take steps within their own organisations to meet requirements.

With respect to data protection and privacy, the Working Group on privacy and data protection of the second phase of the European C-ITS Platform is working out the practical application of the General Data Protection Regulation for (some of) the day-one cooperative intelligent transport systems in Europe. The legal basis for the use of C-ITS data is being investigated. In the first phase of the C-ITS Platform concluded that cooperative awareness messages (CAM) and decentralised environmental notification messages (DENM) are personal data. The aggregation of CAM messages is problematic because the data are personal and, at this point in time, there has no grounds to justify the collection of these data without violating the GDPR. The proposal formulated by the Working Group on data protection and privacy was rejected by Article 29 in June, 2017, meaning that the proposal cannot move forward as is. This point brings forward the issue of “vital interest”, the legal basis for processing data which can save lives on Europe roads. “Vital interest” does not cover CAM messages, but it may cover DENMs.

Access to data is critical to meet the delegated act requirements on safety-related traffic information and real-time traffic information (prirotiy actions c and b of the ITS Directive) and to generate business opportunities. Agreeing to processes to facilitate access to data is being discussed in several groups at the European level (Working Groups data protection and privacy, and Access to Vehicle Information and ACEA). Parties disagree on some points. The discussion focusses on conforming to the regulatory framework (Euro 5/6 Regulation and Type Approval Draft Regulation, eCALL Regulation, art 12.1, ITS Directive and delegated acts, Data protection directive and the GDPR and the Digital Single market strategy and (free flow of) data economy [ACEA, 2017]) while providing access to data. The discussion framework currently focusses on identification of the data under discussion (in this case, vehicle-generated data / operating data), the purpose for which it is being used (road safety, cross-brand services, brand-specific services / component monitoring or personalised services), to determine if and under what conditions parties may have access to the data, and the means of accessing the data.

These active discussions must be kept in mind when reading this report because the outcomes are not yet concrete and the outcomes may affect the conclusions in this report. Road authorities should take part of determine how their standpoint should influence these discussions.

1.2 Document Structure

This document is structured as follows. Section 2 reviews the findings of the use cases and distils actions for National Road Authorities based on these findings. Section 3 investigates the developments in legal sphere relevant for the deployment of C-ITS and distils actions for National Road Authorities based on these findings. Section 4 combines the legal and non-legal findings into a roadmap.

2 Implications of use case analysis using the COBRA+ Tool on actions for National Road Authorities in the short to medium term

2.1 Introduction

The three use cases investigated in Deliverable 5.1, Report on use case results (Malone et al., 2017), form the basis for identification of key actions to be taken by national road authorities in the short and medium term. Each use case addressed specific questions and issues that can support decision-making with respect to Connected and Cooperative Intelligent Transport System (C-ITS) deployment. The issues involved the implications of specific Business Models, the speed at which deployment takes place, the austerity measures taken for existing traffic management (legacy) systems and the simultaneous roll-out of C-ITS and the associated costs and benefits.

Each use case made use of country-specific scenarios. These scenarios included country-specific data and forecasts on the road network, problem size and existing roadside ITS (legacy) systems. The scenarios included the specific parameter choices in the COBRA+ Tool for deployment of C-ITS. These included the choice of service or bundle or C-ITS services, communication platform (cellular or hybrid), the speed of deployment, the use of infrastructure costs savings and the choice of business model. Infrastructure savings arose from the decision of a road authority to scale back legacy systems on the road network while deploying C-ITS. The cellular platform made use of 3G/4G. The hybrid platform included an on-board unit that enables both ITS G5 and cellular communication; both the roadside ITS-G5 units and cellular networks can be used. The outputs of the COBRA+ Tool, Benefit-Cost Ratios (BCR), costs and benefits in different categories, payback period, and percentage of costs of the Road Authority, were used in the analyses.

The scenarios for the Netherlands examined both the full roadway network of the National Road Authority (NRA), Rijkswaterstaat, as well as the C-ITS Corridor in the Netherlands that includes the A16, A58, A2 and A67. The scenarios examined varied the road network analysed, the communication platform, the level of in-vehicle penetration, the percentage of infrastructure equipped for ITS-G5 communication, the service bundles offered, whether infrastructure savings was used or not, and the choice of business model. In total, almost 600 scenarios were analysed.

The scenarios for England examined scenarios for the A2/M2 corridor in England using In-Vehicle Signage. The scenarios were chosen based on consultation with Highways England representatives and reflect Highways England priorities. The scenarios examined varied the communication platform, the level of in-vehicle penetration, the percentage of infrastructure equipped for ITS-G5 communications and the choice of business model. For England, no infrastructure savings resulting from scaling back legacy systems were assumed. In total, twenty-two scenarios were analysed.

The scenarios for Austria examined a section of the European Corridor – Austrian Testbed for Cooperative Systems (ECo-AT), namely the A1 motorway from Vienna West to Linz. The scenarios were decided in discussions with ASFINAG, the manager and operator of the Austrian motorway and expressway network. The scenarios examined made use of the hybrid communication platform and the public business model in which the driver pays for the service, and varied the OEM vehicle penetration (built-in devices), the percentage of infrastructure equipped for ITS-G5 communications and the service bundle. In total, twelve scenarios were analysed.

2.2 Use case findings relevant for short-to-medium-term decision-making

2.2.1 Introduction

The paragraphs below explain relevant findings for the roadmap based on the analyses of the scenarios examined for each use case. The paragraphs cover the choice of communication platform, the extent of legacy systems on the network, results for the corridor vs a full-motorway network, the choice of business model, the choice of services and the use of infrastructure savings.

2.2.2 Cellular vs hybrid communication platform

The choice of platform (hybrid or cellular) affects the Benefit-Cost Ratio (BCR). Holding all other parameters fixed, the hybrid deployment resulted in a slightly higher BCR than the cellular deployment in all cases.

For a given bundle, the hybrid implementation is more effective than the cellular implementation in terms of achieving benefits, but is limited to the area where the ITS G5 roadside units are located. The level of ITS G5 coverage ranged from 5% to 45% in the use cases examined. Additionally, the hybrid implementation has the cellular service available outside the ITS G5roadside unit locations. This means that the hybrid-equipped vehicles always have access to either ITS G5 (with a higher effectiveness for some services) or cellular implementations of the bundle. On the other hand, the costs of the ITS G5 roadside and in-vehicle units need to be incurred. Figure 1 shows the benefits and costs of a cellular (Scenario 1) and hybrid (Scenario 2) implementation, from 2017 to 2030. Note that the figures do not include the in-vehicle capital costs.

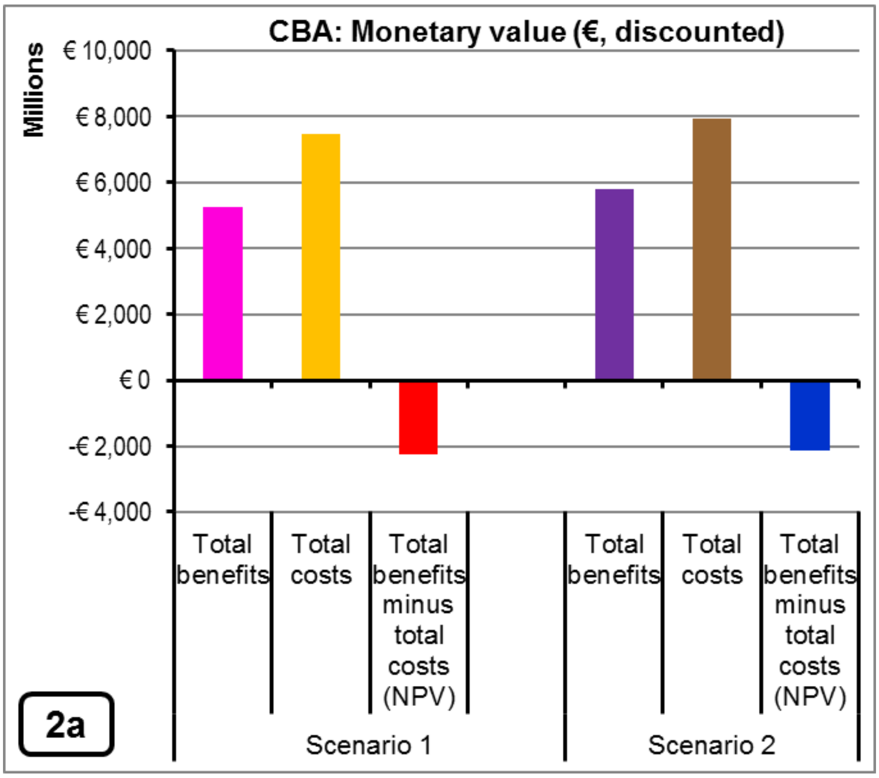


Figure 1: Net Present Value of total benefits, total costs and total benefits minus total costs for Scenario 1(cellular) and Scenario 2 (hybrid), use case the Netherlands

Although the analysis made use of the state-of-the-art impact figures, empirical evidence for the differences in effectiveness between cellular and hybrid implementations is not available. This evidence is needed.

2.2.3 BCR on well-equipped networks with legacy systems

An aspect to consider in calculating and presenting the BCR is the potential cost savings in carrying out traffic management. This aspect can be complex in the case when a country already has a high level of coverage by roadside legacy systems such as Variable Message Signs. The high coverage depresses the Benefit-Cost Ratio due to the overlap of the existing legacy systems and the C-ITS systems. Where there is overlap of legacy systems and C-ITS services, only the marginal benefit of the C-ITS contributes to additional benefits, markedly lower than the full benefits if the C-ITS were to be deployed on roadways with no legacy systems. Thus, in the short term, extra investment costs are incurred on top of the regular operation and maintenance costs of roadside legacy equipment. However, the long-term picture promises overall lower costs of traffic management.

2.2.4 Infrastructure cost savings

Making use of the infrastructure savings option in the COBRA+ Tool has a large positive impact on the BCR in most scenarios. Holding all other parameters fixed, making use of the infrastructure savings in the tool reduces the costs incurred in maintenance and operation of the existing roadside systems. Compared to the business-as-usual scenario, these are benefits: they represent funds that would have been spent in the reference scenario but they are not. However, “turning off” some current legacy systems result in a decrease in safety, increase in travel time, and/ or increase in emissions. The COBRA+ Tool takes estmiates of these unintended disbenefits into account.

Figure 2 shows the business case for the national road authority in two scenarios which are identical except that Scenario 1 makes use of infrastructure savings, and that Scenario 2 does not. Unintended disbenefits are incurred in Scenario 1 (decrease in safety, increase in travel time, etc.). These disbenefits are added to the costs in Scenario 1 in Figure 2. The deployment of C-ITS itself generates benefits that, in this configuration of infrastructure savings and deployment of C-ITS, compensate each other in this case. Overall, Scenario 1 has higher costs, due to the disbenefits; and higher benefits, due to the additional financial savings. The size of the disbenefits are expressed financially in the BCR, but this is an ethical issue as well. If reducing roadside legacy systems does affect societal impacts negatively, should reduction take place? More positively, at what penetration level of roadside and in-vehicle equipment is it safe and ethical to start reducing legacy roadside systems?

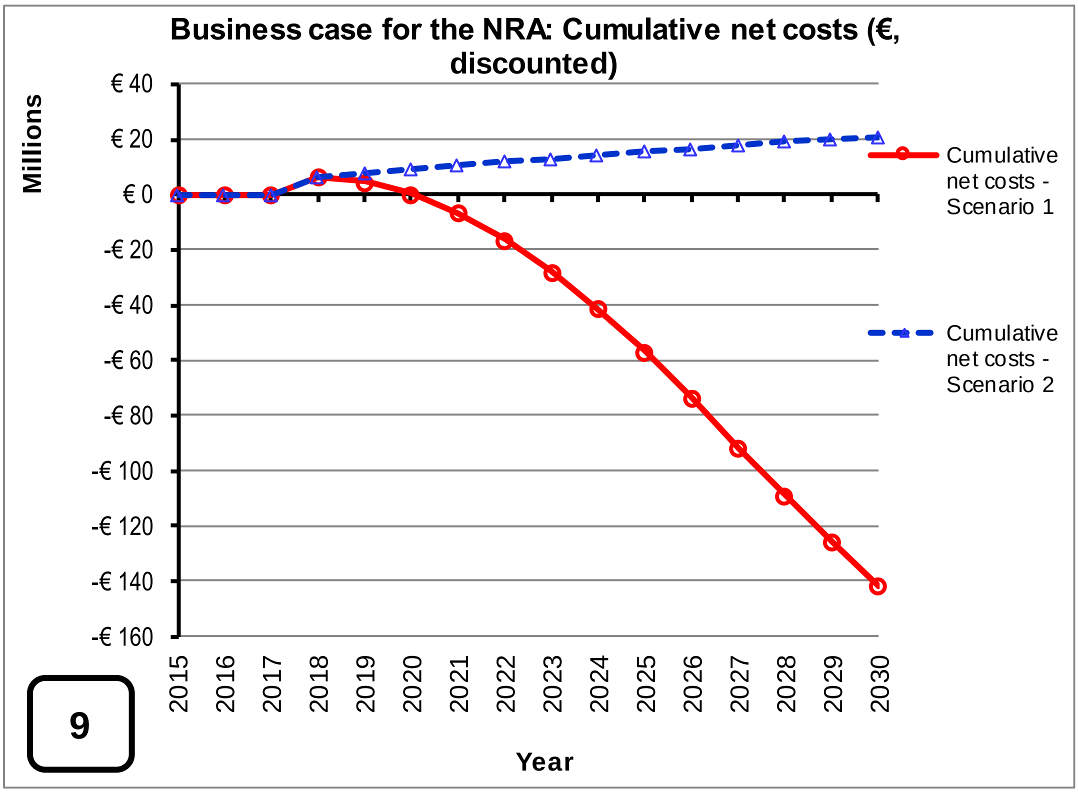


Figure 2: Difference in cumulative costs and benefits with Infrastructure Savings off (Scenario 1) and Infrastructure Savings On (Scenario 2) for a full network and hybrid implementation

2.2.5 Corridor vs full-network

Comparisons between the Dutch corridor and the full road network revealed a consistently higher BCR for the full network for all cellular and hybrid scenarios. Figure 3 illustrates this for one scenario. The C-ITS Corridor, a subset of the full network, has fewer societal problems. The legacy systems cover 100% of the C-ITS Corridor. Thus, deployment of C-ITS on the C-ITS Corridor results in smaller benefits on a per-kilometre basis compared to the full network due to overlap with legacy systems, while incurring the same absolute total vehicle costs (subscription, in-vehicle units) as in the full network. The C-ITS Corridor deployment should thus be seen as a first phase of deployment, with the full potential realised further in the future.

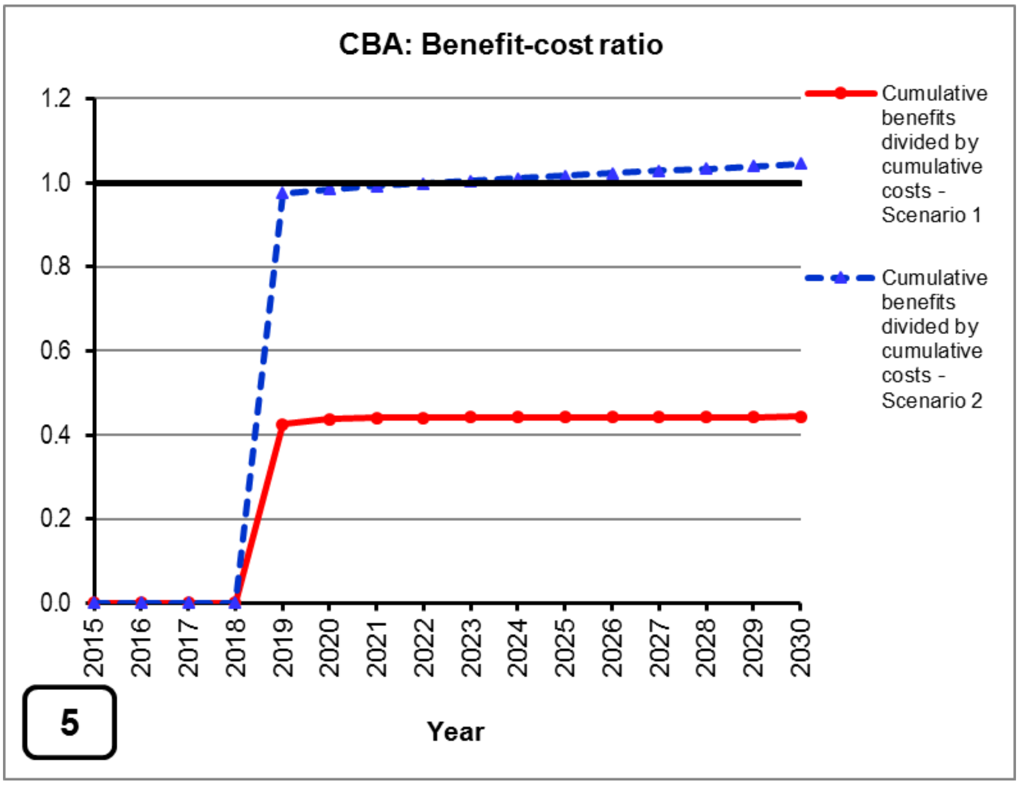


Figure 3: Annual Benefit Cost Ratio on the Dutch Corridor (Scenario 1) vs the full network (Scenario 2) for a hybrid implementation of the In-Vehicle Signage Bundle

2.2.6 Business model choice

The use cases investigated different business models. Both the English and Austrian use cases investigated public models, while the Dutch use case examined the mixed and private business models. The choice of business model immediately affects the costs that the National Road Authority will incur, and thus the payback period for the National Road Authority. The choice of one of the public models means that the National Road Authority is responsible for everything: the National Road Authority takes the responsibility for providing the content and the service; and in the hybrid model, the ITS-G5 roadside infrastructure is purchased, installed and operated and maintained by the National Road Authority. In contrast, the National Road Authority reduces the number of roles it fulfils in the mixed and private models. The National Road Authority reduces its role in the extent of service provision and its role in the ITS-G5 infrastructure (in the hybrid scenario), with the private model reflecting a greater “hands-off” approach by the National Road Authority than the mixed model. However, there is a large difference in realisation of a public vs mixed or private business model. In the former model, the National Road Authority has control over all aspects of the deployment of equipment and service provision. In the latter two models, the National Road Authority does not control all of these aspects. This means that the National Road Authority will work with other stakeholders to achieve the deployment of roadside equipment (in the hybrid implementation) and the content and service provision. Each stakeholder in the chain of delivery of a service must see that it has a win-win situation, crucial to procuring commitment in the chain of delivery. The creation of sustainable business modesl with other stakeholders is a new challenge.

2.3 Implications for the roadmap based on use case analyses: key actions for National Road Authorities

The use cases analyses provide insight into the actions that National Road Authorities can take in the short to medium term (2-7 years) in preparation for deployment of C-ITS. The bullet points below explain these actions.

- **Use the COBRA+ Tool to investigate C-ITS deployment scenarios.** The COBRA+ Tool contains data for Austria, England, Finland, Germany and the Netherlands. Scenarios for Austria, England and the Netherlands have been explored using the tool [Malone et.al., 2017]. Deployment scenarios for Finland and Germany, and Sweden, when the Swedish data is complete, can be carried out. Scenarios need to be defined and run, based on realistic parameter choices for each country in the COBRA+ Tool. Data for additional countries can be added to enable these analyses. For Austria, England and the Netherlands, identify additional issues to investigate based on the current findings. The COBRA+ Tool can assist in developing a strong argument for investment in C-ITS.

- **Investigate cellular vs hybrid implementations of services to get better (empirical) estimates of benefits and costs of these implementations, through support, cooperation with, and participation in pilot and deployment projects.** The state-of-the-art knowledge of benefits and costs of services have been included in the COBRA+ Tool. However, there is little empirical data on benefits, especially the potential differences between cellular and hybrid (ITS G5) implementations. Differences between ITS G5 and cellular communication exist, but the resulting differences in terms of effects using different communication platforms are not empirically documented. For example, communication via ITS G5 has a low latency and better reliability. What is the difference in impacts of service implementation using cellular vs ITS G5 communication? It is assumed that the benefits of using ITS G5 communication will be higher for safety systems, if warnings are time-critical. A cellular implementation has a higher latency. But what is the evidence for these differences in safety impacts? Furthermore, the fact that the benefits of Vehicle-to-Vehicle (V2V) services are not included in the hybrid scenario benefits result in an underestimation of the hybrid scenario Cost-Benefit ratio. Likewise for costs: economies of scale are expected for hybrid systems, but at this point in time this information is not available. Additionally, knowledge of the impacts of bundles of service is needed. It is most likely that services will be deployed in bundles rather than individual services. In addition to impacts, what are the most attractive or likely combinations of services to deploy?

- **Work with stakeholders to assess the feasibility of and realise sustainable business cases.** This recommendation holds for national road authorities that want to pursue public-private or private deployment of C-ITS. A business model is feasible for a national road authority if it is feasible for all actors needed to provide the services examined. What needs to be identified are sustainable business cases for all actors in the value chain. Furthermore, agreement on the governance of service delivery of key (traffic management) services needs to be arranged, especially in an environment when the (public) road operator works with industry and / or service providers to deliver these services. The sustainable business models extend beyond the period of a pilot or project, and are expected to continue for at least a period of a few years.

- **Carry out careful analysis for how to implement infrastructure savings.** Delay the decision for realisation until this analysis is carried out. Infrastructure savings is part of a plan to maintain and improve levels of safety, traffic throughput and environmental impacts while reducing the overall costs. Reducing costs is a benefit, but unintended disbenefits will be incurred. Research is necessary to realize the benefits of infrastructure savings while carefully balancing the disbenefits with the generation of benefits through deployment of C-ITS. This analysis includes deployment of hardware and use of services that are relevant such that infrastructure can be safety removed. Careful analysis of the achieved or required level of C-ITS deployment with the timing of the start of decommissioning and the rate of decommissioning of legacy systems over time needs to take place to ensure that levels of road safety, traffic performance and environmental impacts are maintained and improved. Until such analyses have been carried out, the decision to make use of infrastructure savings should be delayed. Infrastructure savings realised through the reduction of loops (not yet implemented in the COBRA+ Tool) and buying Floating Vehicle Data instead have started to be investigated, but more insight is needed.

- **Follow or take part in developments around 5G**. Given the focus on the study on the decision-making in the next 2-7 years, cellular 5G was not considered. 5G was considered outside the timeframe of this study, due to the uncertainty in the required developments and subsequent standardisation required for the mobility applications. This technology should be followed, investigated and national road authorities should ensure that they take part or are represented in relevant discussions on, for example, standardisation.

3 Legal implications in the short to medium term

3.1 Introduction

3.1.1 Objectives of analysis of legal enablers and hurdles

In order to prepare for the deployment of C-ITS by road authorities, this chapter identifies key actions in the area of legal issues in the short and medium term (2-7 years). These key actions will be based on the three use cases investigated in Deliverable 5.1, Report on use case results (Malone et al., 2017). It takes into account: (i) privacy according to the General Data Protection Regulation (GDPR) – which will apply on May 25, 2018 in all Member States of European Union, (ii) liability according to traffic law and (iii) access to data. These three issues can directly or indirectly be influenced by the National Road Authority with regard to (COBRA+ Tool) service implementation. There are other legal issues, such as criminal law, administrative law, intellectual property and competition law, which are relevant. The budget constraints of the ANACONDA project required that the analysis focus on the three most important legal topics: privacy, liability and access to data.

Given the relevance of collecting and processing (personal) data for the COBRA+ Tool services, either individually or as part of three bundles, Section 3.2 starts with a brief introduction into the relation between (big) data and privacy. In order to support the practical handling of the requirements of the GDPR, this document makes use of RESPECT4U, an approach that captures all relevant dimensions for responsible use of COBRA+ Tool services by road authorities and other interested parties. Based on the inputs of these various building blocks, this section outlines a plan for privacy-respecting data handling by road authorities. This is based upon privacy design strategies. A stepwise approach of these strategies is presented. Paragraph 3.2.2 explains the (changing) nature of where liability lies when parties like the National Road Authorities deploy C-ITS services. If a vehicle is involved in an accident, in almost every jurisdiction, the liability lies at the moment with the driver if it can be shown that the driver is negligent in some way. Paragraph 3.2.3 pays attention to access to data. A key feature of C-ITS services is the amount of data they will generate and the fact that this data will need to be/could be shared with third parties. Yet the data owner will not necessarily want to share that data, or wants some kind of reward for sharing the data. This will create the need for a number of potentially complex contractual relationships that will have to establish who accesses the data, the conditions under which data can be handed over and the financial or business kind of rewards that will be made for that use.

After the analysis of the legal enablers in Section 3.2, Section 3.3 provides insight into the actions that national road authorities can take in the short to medium term (2-7 years) in preparation for deployment of C-ITS.

3.2 Legal Enablers

3.2.1 Privacy regulations

Privacy is a multidimensional concept, meaning different things to different people. One shared perception is the connection of privacy with a sense of freedom/liberty, the freedom to determine for oneself what to share with others. The relevance of such a notion is that it enables individuals to construct their own identity, being free from unreasonable constraints by others. Privacy also refers to other features of a respectful life, such as the dignity of the body, the safe harbour of the home and the secrecy of correspondence. These elements of a dignifying life have been entered in the European Convention on Human Rights, which reflect their relevance for the evaluation of proper behaviour by citizens and organisations. Respect for private and family life complements the relevant perspectives on privacy. Many of these elements are sincerely affected by data processes. The instruments for communication are almost entirely digitized, the home has lost part of its protective walls since we store much of our private activities in ‘the cloud’ and even the body is threatened to be permeated by digital technologies. The concept of privacy thus becomes intimately linked with the concept of the protection of persons with regard to the processing of their data.

For the protection of personal data, some specific regulations are in place. The most relevant of these is the Data Protection Directive (DPD) (95/46/EC) which has recently been replaced by the General Data Protection Regulation (GDPR) (2016/679/EC). The GDPR will enter into force on 25 May 2018. It contains a number of new requirements that are relevant for national road authorities and other parties involved in the chain of delivery of C-ITS services and in due time each party will need to meet these requirements.

The General Data Protection Regulation

The full title of the GDPR is: “Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of their personal data and on the free movement of such data”.

Firstly, the GDPR thus deals with protecting individuals (natural persons). It rules out the protection of organisations, which means that they cannot appeal to the GPDR. Of course, the reputation of organisations can be harmed, but this is covered by other legal regimes.

Secondly, the GDPR relates to personal data, which are defined 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 identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.*”

Different parties in the chain of delivery may process information that falls under this definition. Data such as name, address etc., are personal data. Data that are gathered when people use services as Road Works Warning (short distance), Local Dynamic Event Warning, Traffic Information and Road Works Warning can lead to the creation of personal data, i.e., data that can be related to an (in)directly identifiable natural person.

Thirdly, the GDPR relates to the processing of personal data. Processing is very broadly defined as: “*… any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*.”

This broad definition stipulates the intentions of the legislator: the often-made distinction between ‘having’ data and ‘using’ data with the first being harmless and the second being potentially harmful for privacy (how can the mere possession of data harm the privacy?) is rejected by the legislator. Having data means that these data have been collected and are stored, and both are activities that fall under the jurisdiction of the GDPR.

Last but not least, GDPR applies to controllers or processors who provide the means for processing personal data. Controller means “*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*“. Processor means "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*“.

Figure 4 illustrates the relationship between controller and processor in case of deploying C-ITS services.

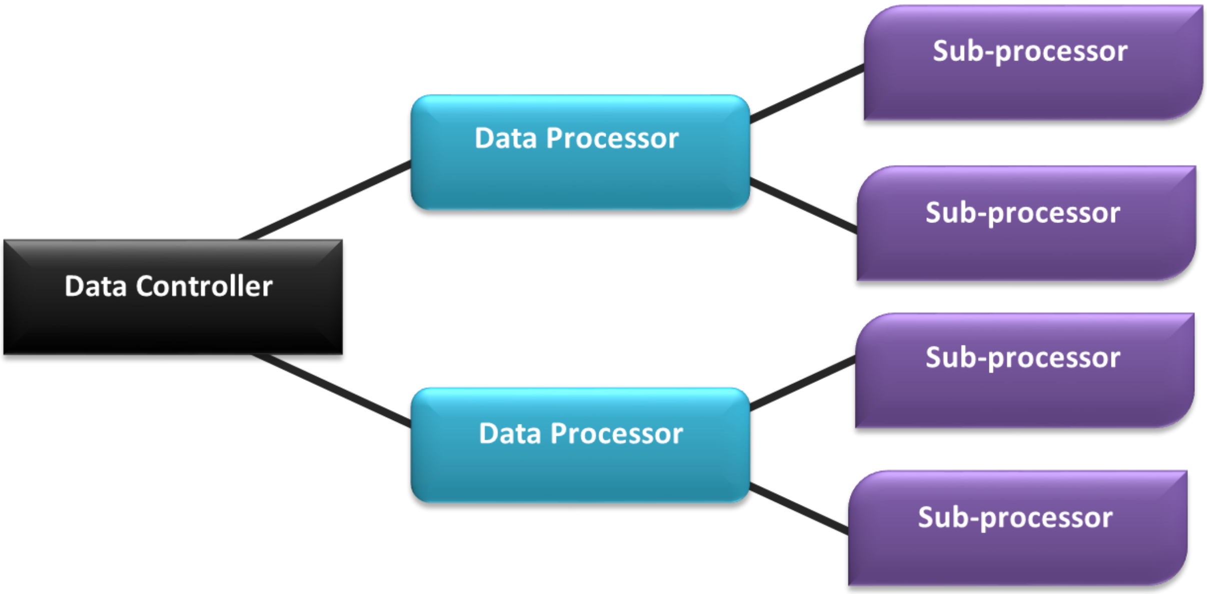


Figure 4: Data controller vs. data processor

Rights of the data subjects

The GDPR acknowledges similar rights to the data subject as was regulated in the Data Protection Directive (95/46/EC) (DPD) (the right to be informed, right of access, right to rectification, right to object). In addition to the right of access, the data subject now has the right to receive a copy of the data undergoing processing. New are the right to be forgotten and the right to data portability. The right to be forgotten is an extension of the right to erasure and is basically a right to request removal from search results. How this right will be exercised in practice is still an open issue, given the intricate complexities of removing all links to specific data (while the data themselves may remain available). The right to data portability is the right to receive all data collected by a controller and having these data transferred to another party. An example of this is the right to request all data that a party has collected during a period on a specific individual and who wants his/her data to be transferred to another party. The GDPR indicates that the requirements for data portability are such that – if possible – data should be directly transferred from one service provider to the other. This is not a strict obligation but if normal business procedures would enable such a transfer, a case can be made that this indeed should be done likewise.

Obligations of the controller and processor

Again, the GDPR attributes obligations to the controller and the processor similar to the ones in the DPD. First, the controller needs to provide legitimate grounds for the processing. Consent is one of those grounds, fulfilling a contract is another. A legitimate interest of the controller itself is a third. Fulfilling legal obligations is a fourth. Any processing must be proportionate (not more than strictly necessary) and should choose the means which are the least obtrusive. Safety measures are prerequisite and must be demonstrable as well.

The GDPR introduces some novel elements as well. The two most relevant ones are the principle of Data Protection by Default/Design and the Data Protection Impact Assessment.

Data protection by default means that the controller should by default introduce measures for data protection. The GDPR names pseudonymisation and data minimisation as two options to provide for data protection by default. A third is the default implementation of settings that serve the privacy of data subjects best, for instance by choosing opt-in instead of opting-out as default setting.

Data protection by design is still a relatively open concept today. No technical and organisational standards have already been accepted that properly outline what needs to be done in order to comply with privacy by design. The phrase '*appropriate technical and organisational measures*' that is introduced in describing data protection by design still lacks substance. A common way of assessing the appropriateness of measures taken is to look at state-of-the-art insights and technologies and whether these have been taken into account. Obviously, more sensitive personal data require better protection than less sensitive data.

A *Data Protection Impact Assessment* (DPIA) is an assessment of privacy risks. It is mandatory in specific circumstances. One of the grounds that warrant the exercise of a DPIA is when profiling is done that may significantly affect the data subject. When specific categories of data are processed a DPIA is mandatory as well. Specific categories of data refer to what usually is labelled as sensitive data: "*data on racial or ethnic origin, on political opinions, philosophical and religious beliefs, on membership in trade unions, on health situation and sex life, on biometrics including genetics*". While non-sensitive data may be processed unless specific limitations apply, sensitive data may not be processed, unless specific conditions are met. Thirdly, a DPIA is necessary when publicly accessible areas are systematically monitored. The elements of a DPIA are under discussion. In the Netherlands, the Dutch government has published a template to be used when performing a DPIA on publicly offered services or systems [website Rijksoverheid].

Case - C-ITS

The legal framework on data protection deals with the tension between data technologies used by government, companies and organisations and the right to privacy and data protection by setting the boundaries within which personal data can be legitimately processed.

So, what is new about using big data? Simply put: it is the scale of big data processing which brings existing privacy risks into a whole new (and unpredictable) level. The development can be described in terms of volume, velocity, veracity, variety, complexity and value of big data but also their combination in analytics. The main privacy challenges associated with Road Works Warning Long Distance could be data sharing between different parties which may request specific measures for secure transfer and processing of data.

Another requirement of the data protection framework is that data controllers (e.g. the national road authorities) must have a clear, specific and legitimate goal for gathering personal data. The goals that are considered legitimate are enumerated exhaustively, both for ordinary personal data and for sensitive personal data – the legitimate grounds for the latter category are stricter. In the Big Data era, though illegitimate by itself, data are often gathered without a specific reason or goal. Only afterwards, may a data controller take the effort of assessing the value of the data and selecting the most valuable data points.

In the case of Road Works Warning Long Distance, the collection of data is widespread and data are gathered from so many sources that service users are often not even aware of the data processes that affect them. There are also significant challenges for the national road authorities to fulfil their duty to inform service users that their personal data are processed and why, because the controller often does not know the identity of the service user nor his contact details. The fact that service users are unaware of the various data processes affecting them and the fact that if they were aware, there may be thousands or more data processes using their personal data also means that it may be challenging for them to assert the various rights they have to control their personal data. The Working Group ion data protection and privacy concluded that cooperative awareness messages (CAM) and decentralised environmental notification messages (DENM) are personal data. The aggregation of CAM messages is problematic because the data are personal and, at this point in time, there has no grounds to justify the collection of these data without violating the GDPR. The principle of "vital interest" does not cover CAM messages, but it may cover DENMs.

Another relevant feature of the GDPR deals with is the aggregation of data in order to create profiles and to explore preferences, attitudes and behavioural features of user services (profiling). The GDPR defines profiling as "*any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*." The most relevant article in the GDPR dealing with profiling is article 22 "Automated individual decision-making, including profiling". This article states that no individual needs to be subjected to a decision which is based solely on automatic decision making, including profiling, if this decision may significantly affect the individual. Such effects could be unjust exclusion of services, or unjust stereotyping of individuals based upon generic features that could be discriminatory. It is not easy to foresee where to draw the line. Price differentiation is allowed, people may be offered different services against different conditions on the basis of specific features. The intent and the outcome of profiling practices need however to be closely monitored. As indicated above profiling practices that may significantly affect individuals warrant the performance of a DPIA. Measures that may be introduced to prevent or mitigate risks could be for example pseudonymisation.

Lastly, an important element is the possibility to combine data sets from many different sources, so as to derive more (and new) information about for example roadworks. Various non-personal data may be combined to infer information related to a person or a group. Similarly, various identifying but non-sensitive data points may be combined to infer a profile or pattern that is sensitive or can be used for practices that have a significant impact on the individual. This may erode the understanding of the concepts of 'personal data' and 'sensitive data'. This trend also requires stricter procedures to delete or anonymize data when no longer needed, because 'anonymous' data face the danger of still being traceable to a person when sufficient additional data are available and the level of anonymization has been too lightly chosen.

3.2.2 Liability regulations

To get a better understanding of a possible impact of C-ITS on liability of road authorities, it is necessary to highlight if and to what extent C-ITS deviates from the current legal situation in the different participating countries.

C-ITS is set up as a supporting service of the road authorities to improve comfort, efficiency and safety of road traffic in the participating countries. It intends to improve efficiency and safety of road traffic by improved real-time traffic information and warnings in addition to the already existing and ongoing traffic information and warnings via road signs, radio and other sources.

Road authorities have the obligation to establish and maintain the necessary infrastructure for road traffic. This infrastructure is organized in local, regional, national or EU-road networks, involving different public authorities (community, department, national and EU-road authorities).

Construction and maintenance of traffic infrastructure is ruled by public law. Product liability rules do not apply to road authorities. Civil law liability of road authorities due to missing, inadequate or unsafe traffic infrastructure or due to missing or false warnings in all participating countries requires the breach of (strictly limited) duty by the competent road authority (notwithstanding the "political liability" for a lousy performance, enforced during the next election). In addition, the liability of the road authorities is of a secondary nature, as the driver of a vehicle has the prior-ranking, unconditional duty to keep his vehicle under control and to prevent accidents under all circumstances. Irrespective of the quality of the road infrastructure or the available traffic information, the driver always must adapt his driving to the current traffic situation. Road signs and traffic information are to be understood as information to support the driver in fulfilling this duty. If the quality of the road infrastructure is poor or the situation unclear (e.g. due to weather conditions or unclear/missing road signs), the driver must appropriately react or slow down in order to avoid any accident. Therefore, the road authority would run a risk of liability only by negligently providing wrong information on or not warning of a situation that the driver could not foresee and not handle appropriately. As such situations are rare (e.g. all traffic lights are giving way at the same time, thereby causing an accident), the risk of liability for a road authority currently is low.

As false information on traffic flow or false/missing warnings already today do not trigger liability of road authorities, (real-time) improvement of such information or warnings (Local Dynamic Event Warnings and Traffic Information and Road Works Warning Long Distance) should not result in additional liability risks.

The same applies to In-Vehicle Signage (Bundle 2), as a (wrong) speed limit does not entitle the driver to speed accordingly, on the contrary he must adapt his speed to the given traffic situation irrespective of the applicable speed limit. In case of a complete replacement of current road signs by In-Vehicle Signage instead of adding on, the road authorities would have to ensure that every road user is able to receive the relevant information and warnings real-time. In case the road authorities should involve subcontractors or cooperation partners to realize In-Vehicle Signage, this will not change the (final) responsibility of the road authorities for the appropriate information and warning of drivers. Therefore, detailed ruling on the scope of supply and services as well as on appropriate liability should be included in the respective contracts with such cooperation partners. Regarding enforcement of speed limits, the burden of proof would change insofar as up to now, the driver had to prove that there was no visible road sign (what he usually could not achieve), whereas now the public prosecutor would have to prove that the driver has received the applicable speed limit, but nevertheless exceeded it. In case of a deviation between the speed limit shown by a road sign and the one shown by the In-Vehicle Signage, additional law is needed to regulate which system should be considered the most relevant one.

3.2.3 Access to data

Access to data and the associated ability to retrieve data within a repository has been investigated in data management literature since the beginning of the century. As far back as in 2002, data ownership as both the possession of, and responsibility for, information is considered as elements of access to data. In this respect not only does access to data include the ability to create, modify, package, derive benefit from, sell or remove data, but also the right to assign directly to "the intrinsic value of data, as well as their added value as a by-product of information processing".

Data ownership's prominence in the data management debate and its centrality in economic, and business circles has contributed to put it at the core of policy discussions. In its interim synthesis report on "Data-driven for Growth and Well-being", the Organisation for Economic Co-operation and Development (OECD) maintains that "data ownership and control of data" is fundamental to ensure that the data-driven economy is granted sufficient and effective resources adding that governments and public agencies should promote better access and free flow of data across the economy as a whole and not only over the public sector [OECD website].

Although commentators and contracting parties frequently discuss the issue in terms of *'data ownership'*, this is misleading since few jurisdictions other than certain states in the USA have laws that treat data as a form of property. Legally speaking, to own something means to have property rights in it: that is, the rights of possession, use, and enjoyment, which the owner can bestow, collateralise, encumber, mortgage, sell, or transfer, and the right to exclude others from. The point is more than mere semantics: legal categorisation as property would automatically define the owner's privileges, including the ability to enforce terms for third party access and use, and dictate the legal mechanisms for transaction. Accordingly, a mistaken assumption that data is property may for example lead to reliance on covenants for title and equivalent statutory provisions which do not, in fact, apply.

Legal context

The EU legislative acquis contains a number of instruments of relevance for assessing data localisation requirements in national law. The GDPR provides for a harmonised and high level of protection of personal data and is the foundation for the free flow of personal data in the EU. Furthermore, the GDPR bans prohibitions or restrictions to the free movement of personal data for reasons connected with the protection of natural persons with regard to the processing of personal data. Restrictions justified by other reasons than the protection of personal data, e.g. under taxation or accounting laws, are thus not covered by the GDPR. Furthermore, non-personal data remain outside the scope of GDPR. Restrictions to the storage or processing of non-personal data and restrictions to the storage and processing of personal data justified by other reasons than the protection of personal data therefore need to be assessed on the basis of other EU legal instruments, namely:

- Secondary legislation giving effect to the Treaty [Official Journal *C* 326/47 of 26.10.2012] provisions on the free movement of services and the freedom of establishment that includes Directive 2000/31/EC, which bans restrictions to the freedom to provide information society services from another Member State and prohibits Member States to make the taking up and pursuit of the activity of an information society service provider subject to prior authorisation or any other requirement having equivalent effect [Directive 2000/31/EC].
- Similarly, Directive 2006/123/EC deals with authorisation schemes and other requirements regulating access to, or the exercise of, a service activity and contains provisions both to ensure the right of providers to provide services in a Member State other than that in which they are established and to prevent Member States from imposing on a recipient requirements which restrict the use of a service supplied by a provider established in another Member State [Directive 2006/123/EC].
- Finally, Directive 2015/1535 puts in place a mechanism aimed at preventing the adoption by Member States of rules on information society services, including data storage or processing services, that may create obstacles to the free movement of services in the internal market. According to the Directive, the Commission and the Member States may submit a detailed opinion to the Member State notifying a draft measure to raise concerns on aspects that may hinder the free movement of services [Directive (EU) 2015/1535].

3.3 Implications for the roadmap based on legal analyses: key actions for National Road Authorities

3.3.1 Introduction

The legal constraints which we presented in the preceding paragraph are just one part of the conditions the involved parties could explore in order to meet privacy expectations of its customers (service users). They are relevant and fundamental to any data processing activity they organise. But other conditions need to be fulfilled as well, such as the manner in which for example national road authorities want to involve the customer/service user in the data processing. The actions that national road authorities can take in the short to medium term (2-7 years) in preparation for deployment of C-ITS are provided in Sections 3.3.2 - 3.3.4

3.3.2 Putting privacy regulations into practice

- **Investigate privacy design strategies in the data value chain:** an overview of strategies for designing privacy is offered by some recent reports and publications. These design strategies encompass four approaches that elaborate data protection in data processing activities (SEPARATE, AGGREGATE, MINIMISE and HIDE), two strategies directed at enabling organisational actions to data protection (DEMONSTRATE and ENFORCE) and two strategies focusing on the relationship with the data subjects: INFORM and CONTROL. Figure 5 and Table 1 illustrate and explains these strategies briefly. When looking into the value chain of data analysis, it is important to take into account the purpose of each of the phases and the standpoints of all parties involved therein (data subject, different data controllers and processors, third parties). In this way, it is possible to extract the specific privacy requirements and the relevant implementation measures per phase. Still, it is important to note that apart from the needs of each particular phase, it is essential to implement a coherent approach to data protection, taking into account the complete lifecycle of the analytics. Therefore, it is not just about one technology or another, but rather about the synthesis of many different technologies adequately addressing all the needs of the different data processing nodes.

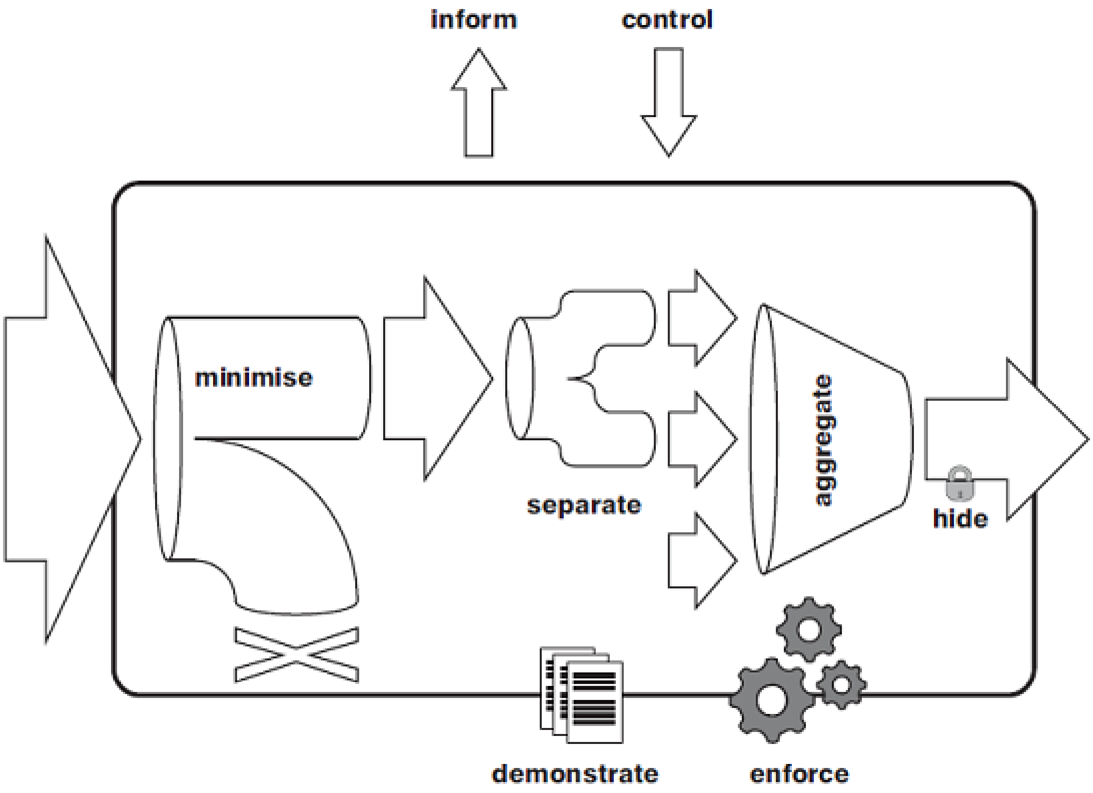


Figure 5: Privacy by design strategies

Table 1: Privacy by design strategies

	Privacy by design strategies	Description
1	MINIMISE	The amount of personal data should be restricted to the minimal amount possible (data minimisation).
2	HIDE	Personal data and their interrelations should be hidden from plain view.
3	SEPARATE	Personal data should be processed in a distributed fashion, in separate compartments whenever possible, separating identifying data from non-identifying data.
4	AGGREGATE	Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.
5	INFORM	Data subjects should be adequately informed whenever their data are processed (transparency).
6	CONTROL	Data subjects should be provided agency over the processing of their personal data.
7	ENFORCE	A privacy policy compatible with legal requirements should be in place and should be enforced.
8	DEMONSTRATE	Data controllers must be able to demonstrate compliance with privacy policy into force and any applicable legal requirements.

- **Carry out a Privacy Impact Assessment:** one very important privacy principle directly related to the data collection phase is that of data minimisation. Each data controller who is collecting the data needs to precisely define which personal data are actually needed (and which are not needed) for the purpose of the processing, including also the relevant data retention periods. Specific processes should be in place to exclude unnecessary personal data from collection/transfer, reduce data fields and provide for automated deletion mechanisms. Privacy Impact Assessments (PIA) can be valuable tools for data controllers, in order to define the exact data processing needs limiting data to what is absolutely necessary for a certain purpose. Another aspect which may come even as a result of the PIA, is when aggregated information is used instead of personal data. Indeed, in certain cases, such as in statistical analysis from distributed sources, the personal data might not even need to be collected in the first place and the collection of anonymised information might be sufficient. Local anonymisation (or anonymisation at source) is the most prominent solution, which could allow the individual (or a controller processing data for the individual) to remove all personal information before releasing the data for analysis.

- **Investigate privacy enhancing technologies:** in many cases information about the individual may be collected without him/her even being aware. Privacy enhancing technologies could be anti-tracking, encryption, identity masking and secure file sharing tools. Another prominent technique is that of anonymisation. Different privacy models and anonymisation methods are in place to preserve data inference, for instance in statistical disclosure control and privacy preserving data mining techniques, including association rule mining, classification and clustering. K-anonymity and differential privacy are the two main families of privacy models with different types of implementations.

- **Develop transparency tools**: the individuals need to be adequately informed about the collection of their personal data for data anlaysis. To this end, appropriate information notices and other transparency mechanisms should be in place. Such tools should be available to the individuals throughout the data processing (and not only the collection). Still, the point of collection is the most important point for the individual in order to make an informed decision about the use of his/her personal data.
- **Develop empowerment tools**: again, the collection phase is the phase where the consent of the user needs to be obtained (if this is the legal basis for the processing). Practical and usable implementations of opt-in mechanisms are crucial in this regard. Moreover, opt-out tools should be offered to the individuals at any point of the processing. Other mechanisms providing user control, such as sticky policies and personal data stores, are important measures to explore.
- **Establish privacy governance**: adopting a privacy-respecting data handling needs to be done in a thoughtful and stepwise manner. This report is already the first step of this process. This bullet proposes to continue with a strategy of small steps, enabling evaluation of technical, organisational and business features in every stage of the implementation process (see Figure 6 and Table 2). Given the focus on customers, it is recommended to establish a customer panel to guide the initial steps of the development of the dashboard. A steering group could be necessary in which the national road authorities that either deliver information/control or are affected by potential choices of customers are represented. Given the relation with the GDPR, the Data Protection Officer should be part of the steering group as well. A frictionless integration of the privacy dashboard with the databases requires sufficient time and expertise to design the required interfaces. The measures in the governance model must be reviewed at regular intervals and when there are sudden changes in the organisation. This could, for example, be related to the purchase of new systems or devices, the implementation of new processes, the merging with other entities or the forging of new partnerships with third parties. All changes are potentially significant to the way an entity processes personal information and therefore the changes will be incorporated into the governance model.

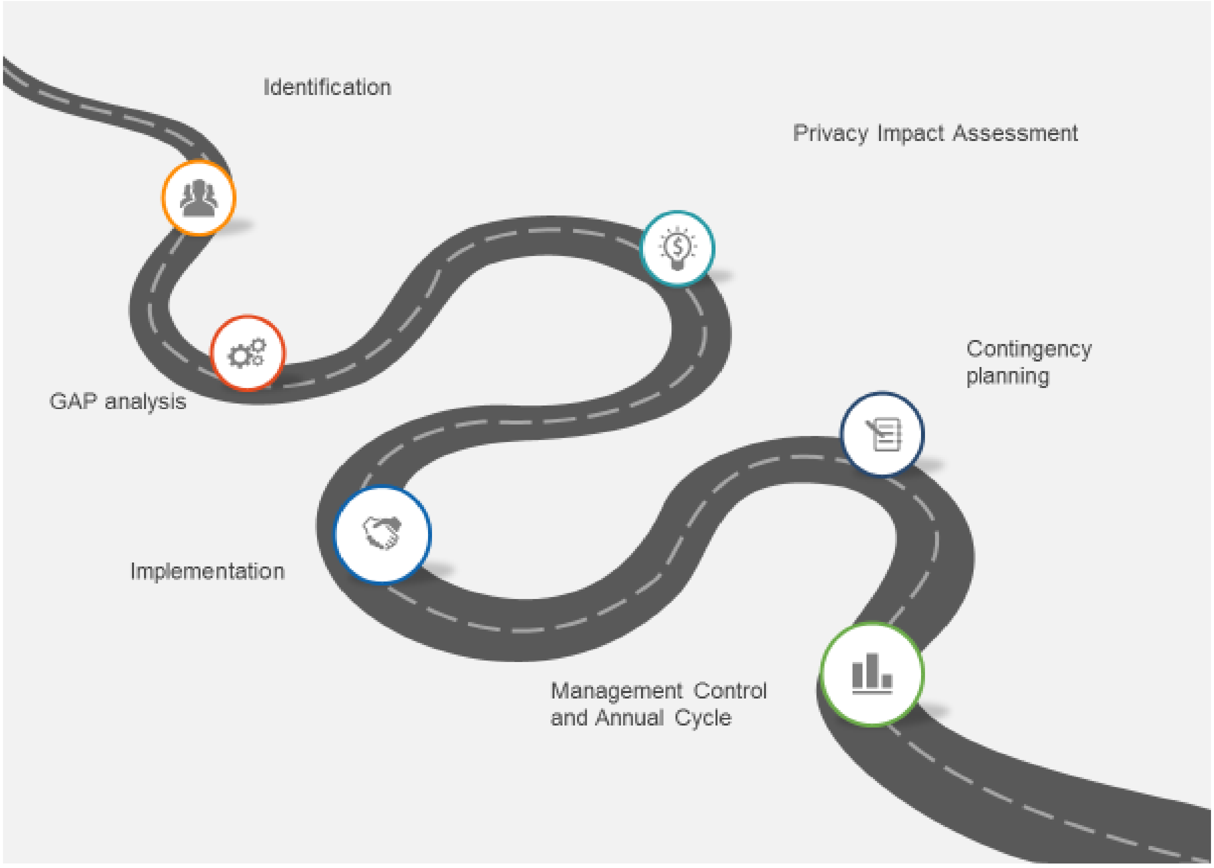

Identification
Privacy Impact Assessment
GAP analysis
Contingency planning
Implementation
Management Control and Annual Cycle

Figure 6: Implementation of compliance in 6 steps

Table 2: Compliance in 6 steps

	Phases	Description
1	Identification and data flow analysis	In this phase, national road authorities define what the organisation's core activity actually is. This encompasses such things as a mapping of all the data: As part of the identification phase, the national road authorities shall produce a so-called data flow analysis. The outcome of the identification phase shall be a complete overview of the personal data, and of the systems, processes and people that handle them.
2	GAP-analysis	In this phase, the results of the identification phase are compared with the requirements set out in the GDPR, so that it is clear as to what gaps the national road authorities have with regard to complying with the regulation. The result of a GAP analysis is not only a roadmap for future initiatives. The analysis can also reveal if, for example, there are fundamental security conditions that must be addressed first before one can more directly comply with the requirements in the GDPR.

3	PIA	The purpose of a PIA is the main privacy risks for the data subjects are inventoried and that mitigating measures are considered and proposed.
4	Implementation of action plans	Implementation phase is highly individual and it depends on the overall digital maturity level. Regardless of size and maturity level, it is required that national road authorities are able to document at all times that they are compliant with the GDPR. Compliance is regarded as an ongoing quality-control measure of its own processes.
5	Contingency planning	In cases where a leak of sensitive information occurs, the GDPR contains a new requirement that an organisation must inform the relevant authorities within 72 hours of the data leak being registered. Seen in this light, 72 hours is a very short response time. Therefore, one needs to be at the forefront of any data leakage and prepare in advance a contingency plan that can take effect immediately. The plan should describe in detail who within the national road authority shall be responsible for doing what.
6	Ongoing management	The work with the GDPR is not a job with a fixed date of completion. It is to be considered as an ongoing assurance that the national road authorities can always document that it has been conscientious with regard to the protection of the registered party's personal data. Therefore, it makes the most sense to concretise the work of the GDPR as an ongoing process. For example, it might call for applying the governance model (indicating the tasks associated with auditing and inspection, risk management, policies and resources) into an annual cycle. The annual cycle ensures, among other things, that the national road authorities carry out the necessary actions in the action plan, and that it can demonstrate that it complies with the new measures.

There are different privacy governance models. One of the most comprehensive model has been developed by TNO/PI.lab, which combines the key elements of behaving privacy respecting in one encompassing perspective: RESPECT4U (Figure 7 and Table 3).

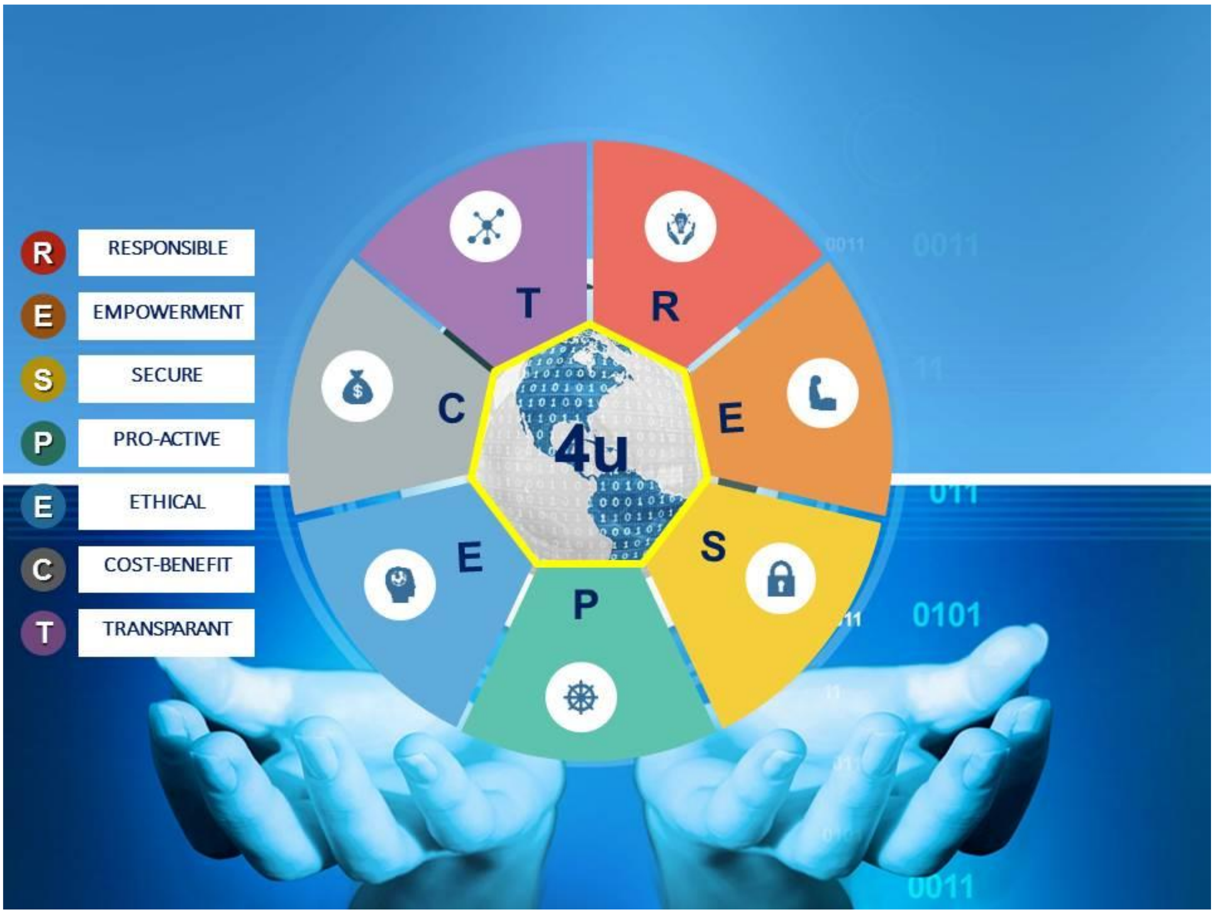


Figure 7: RESPECT4U (©TNO/PI.lab)

The various dimensions of RESPECT4U offer an encompassing perspective of what organisations involved in providing a service including national road authorities can do to enhance the awareness for privacy within the organisation while simultaneously demonstrating this awareness to the customers it serves. All dimensions of RESPECT4U are relevant for the national road authorities and the parties involved.

Table 3: RESPECT4U

Building block	Description
Responsible	Label indicating the willingness of the organization to act responsibly.
Empowerment	The data subject is offered tools to exercise control over data collected and processed by the organization that refer to him/her.
Secure	The data processing obeys standard security practices, uses state of the art encryption techniques and secures access and use of data
Pro-active	The organization has established a routine to systematically and structurally take privacy as a design parameter into account. It uses tools such as a DPIA to pro-actively inventory risks.
Ethical	The organization is aware of societal implications of its data processing activities and has implemented safeguards to explore and mitigate potentially negative impacts.

Cost & Benefit	Trying to engage with a cost-benefit analysis, one needs to address costs and benefits in a comparative manner.
Transparent	The organization has established procedures for the processing of (personal) data to indicate processes, roles, responsibilities with respect to data handling activities, both within and external to the organization.
4U	One is a person, two is a relation, three is a crowd, four is society. RESPECT4U captures them all.

3.3.3 Putting liability regulation into practice

- **Specify the quality of the data and services to be provided**: In case road authorities intend to engage in new business models based on traffic data, they should specify the quality of the data and services provided in detail and carefully define their contractual obligations combined with a set of buyer’s duties to verify the data received prior to its use in order to reasonably limit their liability.

- **Establish agreements on the generation and quality of data**: in particular providing traffic data by road authorities to third parties for the realisation of highly- or fully-automated driving functions requires a detailed prior agreement on the generation and quality of such data, on the intended use of such data as well as on concepts to ensure compliance with data protection and data security requirements in the given application; furthermore, who will be responsible for the transmission and verification of these data; and finally, a reasonable limitation of the liability of the road authority must have been carefully worked out in detail and agreed prior to the first use of such data in the automotive application.

3.3.4 Putting access to data regulations into practice

- **Examine existing Intellectual Property (IP) schemes:** take a look at existing IP schemes regarding the extent to which they could cover data as such.

- **Establish measures for access to data**: although the protection of trade secrets and know-how shows some features of property, it is based on factual secrecy. Protection depends on technical, organizational, as well as contractual measures sufficient to preserve the confidential nature of the information.

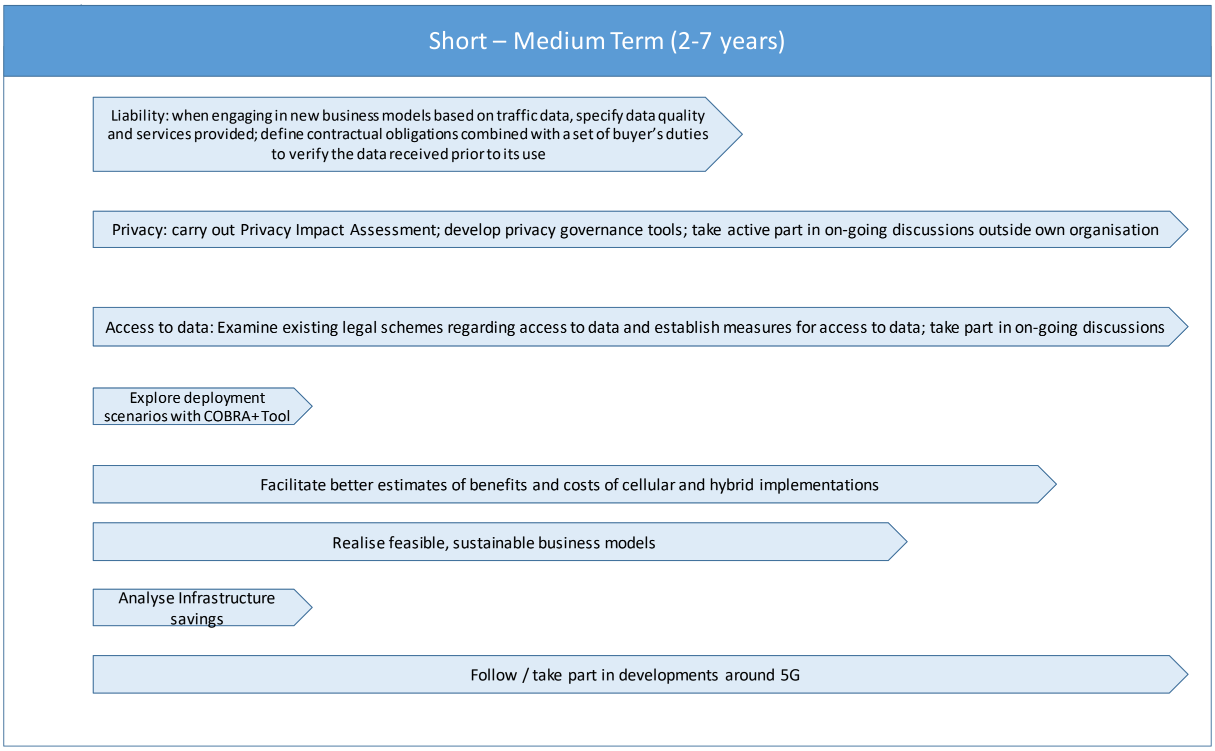
4 Summary and Roadmap

Two sets of analyses provide input to the identification of the actions needed to be taken in the short-to-medium term by National Road Authorities. The first set comes from the application of the COBRA+ Tool to Austria, England and the Netherlands. These use cases are documented in Deliverable 5.1, “Report on use case results” [Malone et. al., 2017]. The second set of analyses, addressing the three most pressing legal issues, is contained in Section 3 of this report.

Figure 8 provides an overview of the actions. The arrows name the actions. The arrows start at the left-hand side of the diagram, the time of the writing of this report, and stretch into the future to the right. The length of the arrows is relative. The shorter arrows represent activities that have a shorter timeline. The longest arrows indicate an activity which is on-going or for which it is unclear when it will be completed.

The analysis of the impact of C-ITS on the liability of the National Road Authority revealed that the impact is not significantly different from current activities that National Road Authorities carry out, assuming that C-ITS is provided in addition to traffic information and road signage as provided today. The primary activity with respect to C-ITS is, in the case that National Road Authorities intend to engage in new business models based on traffic data, that they should specify the quality of the data and services provided in detail and carefully define their contractual obligations combined with a set of buyer’s duties to verify the data received prior to its use in order to reasonably limit their liability.

Privacy is a hot topic not only in C-ITS but in many areas. With the General Data Protection Regulation (GDPR)(2016/679/EC) entering into force on 25 May 2018, it brings a number of new requirements for National Road Authorities and other parties involved in the chain of C-ITS delivery. The implications are broad-ranging and require action by National Road Authorities both before and after 25 May 2018, some of which are on-going.



Short – Medium Term (2-7 years)

Liability: when engaging in new business models based on traffic data, specify data quality and services provided; define contractual obligations combined with a set of buyer's duties to verify the data received prior to its use

Privacy: carry out Privacy Impact Assessment; develop privacy governance tools; take active part in on-going discussions outside own organisation

Access to data: Examine existing legal schemes regarding access to data and establish measures for access to data; take part in on-going discussions

Explore deployment scenarios with COBRA+ Tool

Facilitate better estimates of benefits and costs of cellular and hybrid implementations

Realise feasible, sustainable business models

Analyse Infrastructure savings

Follow / take part in developments around 5G

Figure 8: National Road Authority roadmap for deployment of C-ITS fort he short-medium term

The proliferation of data brings new issues related to the free movement of services and the freedom of establishment, the right to provide services and the absence of obstacles to the free movement of services in the internal European market. The action related to data is to ensure access to data and to establish the measures to access the data. Take part in on-going discussions on data access with respect to data outside National Road Authorities'' own organisations.

The remaining actions in the short-to-medium term concern the preparation of decisions to be made for C-ITS deployment. There are many parameters in deployment: how much of the network to equip, when to start with equipment, which communication technology to use and when is it feasible to reduce the existing roadside infrastructure (infrastructure savings)? These all can be investigated in scenarios using the COBRA+ Tool, to prepare the decisions to be made and to identify areas for deeper analysis using more detailed information or models.

Separate from the tool are the realisation of business models, resulting in some cases in contracts and relationships with third parties who invest in, operate and / or maintain elements of the C-ITS. In many cases, relationships have been established during projects with a defined end-date in which the National Road Authority or other public authority funds some or all the activities. In some cases, the funding is not the desired post-project business model.   Actions need to be taken to realise sustainable, post-project business models. The C-ITS Platform Working Group on horizontal issues (Business Models) has taken steps in defining actions ot support Business Model deployment, which Road Autnorities can use.

Finally, 5G is a communication technology not considered in the ANACONDA project in which this work was carried out. National Road Authorities should actively follow developments to position themselves to follow 5G technical, standardisation and security developments to position themselves for a decision to integrate it into future C-ITS deployment.

5 Glossary and definitions

Aftermarket	In-vehicle device fitted after purchasing the vehicle, usually permanently connected to the vehicle's systems
BAU	Business As Usual
BCR	Benefit Cost Ratio
BM	Business model
CAPEX	Capital costs of equipment to support a service
CBA	Cost Benefit Analysis
Cellular network	Communications platform to support long range communications e.g. mobile phone
DPD	Data Protection Directive (95/46/EC)
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation (2016/679/EC)
ITS	Intelligent Transport System
Managed motorways	An integrated set of traffic management systems to improve traffic flow and road capacity; in the UK they primarily involve variable speed limits and hard shoulder running.
NPV	Net Present Value
NRA	National Road Authority
OECD	Organisation for Economic Co-operation and Development
OEM	Original Equipment Manufacturer (e.g. vehicle manufacturer)
OPEX	Operational costs of running or using a service
Payback year	The first year in which the cumulative benefits of a service exceed the cumulative costs invested in it
Penetration rate	Proportion of vehicles which are equipped to participate in a service
PIA	Privacy Impact Assessment
Queue protection	Automatic traffic management system used to detect sudden traffic disruption and warn traffic approaching the scene to protect vehicles at the back of the queue from rear-end collisions
Smartphone	Mobile telephone used to deliver a variety of other services to users, via Apps
Unintended impact	Dis-benefits occurring as a result of the cooperative system. In calculating the benefit: cost ratio in the tool, these are treated as if they were additional costs
VMS	Variable Message Sign to display a number of messages, and which can be switched on or off as required; various types of sign are available involving different technologies and costs. It is assumed here that these are large signs which can provide several lines of text and colour graphics, providing the existing infrastructure for information delivery for all of the three bundles of services considered here: warnings, speed limits, travel information and route guidance

Wireless beacon	Communications beacon to support short range communications between vehicles and the roadside. It is assumed that each beacon has a range of 300 metres.

6 References

ACEA (2017), presentation „Access to Data for Third Party Services“, C-ITS Platform Working Group on Horizontal Issues: Business Models, Brussels, 13 June 2017.

Cellular roaming charges (March 15, 2017). http://europa.eu/youreurope/citizens/travel/money-charges/mobile-roaming-costs/index_en.htm

Consolidated version of the Treaty on the Functioning of the European Union [Official Journal *C* 326/47 of 26.10.2012].

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [Official Journal *L* 178 of 17.07.2000].

Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market [Official Journal *L* 376 of 27.12.2006].

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [Official Journal *L* 241 of 17.09.2015].

European Parliament and Council Directive 95/46/EC, 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data [Official Journal *L* 281 of 23.11.1995].

Malone, K., A. Soekroella, F. Ognissanto, J. Hopkin, A. Stevens and P. Nitsche (2017), Report on use case results. ANACONDA Deliverable 5.1.

OECD website (April 7, 2017), http://oe.cd/bigdata.

Ognissanto, F., J. Hopkin, K. Malone, A. Soekroella, I. Erdelean and P. Nitsche, (2017). COBRA+ Tool User Guide, ANACONDA Deliverable 3.2.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [Official Journal *L* 119 of 04.052016].

Website Rijksoverheid (April 7, 2017), https://www.rijksoverheid.nl/documenten/publicaties/2013/06/24/toetsmodel-privacy-impact-assessment-pia-rijksdienst.