ITS Action Plan

FRAMEWORK CONTRACT TREN/G4/FV-2008/475/01

ITS & Personal Data Protection
Final Report

Amsterdam, October 4th, 2012
20121004_ITS AP5 1_D5 Final Report v1.0 SEI.docx

EUROPEAN COMMISSION
Directorate-General Mobility and Transport
Unit C3
Rue J.-A. Demot 28, 04/68
B-1040 Brussels
Belgium

Stefan Eisses
stefan.eisses@rapptrans.nl

Tom van de Ven

Alexandre Fievée

VERSIONING AND CONTENT REVIEW INFORMATION TABLE

Version number	When	Changes / update	Author (Organisation name)	Reviewer (name of reviewer and organisation)
1.0	04/10/2012	Final for EC review	Stefan Eisses (Rapp Trans NL)	Tom van de Ven (Rapp Trans NL)

Management Summary

Background and Scope

Intelligent Transport Systems (ITS) can significantly contribute to a cleaner, safer and more efficient transport system. A legal framework, the ITS Directive, was adopted in 2010 to accelerate ITS deployment across Europe. It noted that the further deployment of ITS, in spite of all its benefits, may create new or intensified challenges to the protection of privacy and personal data of people when travelling from one place to another.

Under the framework contract "Technical, Legal and Organisational Support for the Implementation of the ITS Action Plan", a study was commissioned to “Assess the security and personal data protection aspects related to the handling of data in ITS applications and services and propose measures in full compliance with Community legislation”. The objectives and key questions of this task (5.1) have been defined by the EC in the following way [1]:

The objectives of this study are to:

1. Assess the importance and impact of data protection and privacy aspects in the areas and actions of the ITS Action Plan and ITS Directive
2. Evaluate which potential measures could be undertaken and make recommendations for further action.

These objectives lead to the following key questions to be answered by the study:

1. What is the state-of-the-art concerning security and personal data protection aspects related to the handling of data in ITS applications and services in Europe?
2. In particular, which measures, rules and procedures exist or have been applied so far to deal with the data protection issues of ITS applications and services?
3. What ITS applications, or types of ITS applications, are the most subject or prone to data protection issues, or would require specific measures to address those data protection issues? Why is it so?
4. Which specific measures (legal, technical, organizational) would be required to guarantee the protection of personal data in ITS applications or services, while not prohibiting the development of novel applications and services?

This report constitutes the final report of the study.

Approach

Through desk research, documents concerning relevant legislation, case law, opinions and advices from stakeholders and research and standardisation results were collected and analysed. A number of stakeholders were invited to provide points of view, to share practical experiences and to suggest further documents of relevance.

In consultation with the EC, 10 ITS applications/application areas were selected for a more detailed analysis. The selection was based on the current or expected scale of deployment of the application and the (potential) impact on user privacy. Also the diversity between the selected applications was deemed important. As a rule, from different applications with close resemblance in terms of data and architecture, only one was selected. This approach led to the following set of 10 applications:

- Digital Tachograph
- eCall
- Road User Charging
- E-ticketing in public transport
- Parking Payment services
- Pay-As-You-Drive insurance
- Section Speed Control
- Fleet Monitoring
- Traffic Data Collection
- Cooperative Systems.

The general principles of the data protection directive were applied in the context of these applications, and results addressing data protection in the specific application context were discussed.

General Findings

17 years after the adoption of the data protection directive, 95/46/EC, it may be concluded that its concepts and principles have proven to be a stable and useful legal basis for personal data protection in the EU. The national legal implementations and practice of data protection have nevertheless led to a fragmentation in the application of personal data protection across the European Union. It is also observed that developments in the area of computing, internet, mobile communications, social media and their widespread use by consumers pose new challenges for personal data protection. The existing framework is not fully adequate/effective to cope with these challenges.

On 25 January 2012 the Commission presented a new legal framework for personal data protection in the EU. This is currently discussed by the co-

legislators; the European Council and the European Parliament. Its aim is not to change the objectives and principles, but to remove the inconsistencies and inefficiencies of the current constellation. With respect to harmonisation, refinements to the definition and rules for 'unambiguous user consent', 'the right to be forgotten' and liability of the processor are expected to improve legal certainty for both controllers and data subjects. Enforcement is expected to become more effective as sanctions will have to be specified for different categories of data protection regulation violations. Efficiency is expected to be gained by reducing the administrative burden for processing situations that have limited privacy risks whilst at the same time imposing higher administrative requirements on high-risk processing situations. The rules for transfer of personal data to third countries are simplified as a prior authorisation is not required anymore where a transfer is based on standard data protection clauses or binding corporate rules. These modifications are of course not specific for ITS, but the areas of improvement certainly apply to many services in that area.

Sector-Specific Guidelines

Both in the existing and proposed new legal framework, a fundamental question is what additional sector or application specific rules and methods (whether mandatory or self-imposed) are useful to improve data protection in ITS applications. Whereas specific guidelines might increase clarity and consistency within an application area, significant differences in objectives, users groups, size and scope between deployments render it challenging to formulate specific solutions or constraints that would apply to all situations. Formulating guidelines on a higher level of abstraction can be useful but has the risk of adding little value to the legislation itself.

When schemes are introduced that affect large groups of private users and that have a mandatory element, e.g. in the area of passenger car road pricing or e-ticketing, arrangements for personal data protection are often subject to public debate and of political importance. As a consequence, the outcomes in one country are not fully predictable and not necessarily consistent with outcomes in another country. The trade-off between important interests such as efficiency, enforcement/fraud prevention, flexibility, ease of use and user privacy is never absolute and in such cases made in the political domain.

Analysis of Applications

The assessment of 10 different ITS applications allows for some interesting observations:

- Some applications have had abundant coverage by dedicated opinions concerning the data protection issues involved. Other areas much less. This is not always in relation to the privacy risks involved.

- In the perception of the user, as well as in the legal basis, there is a clear distinction between services (or elements of it) an individual chooses or agrees to out of free will, and things he is forced to accept because there is simply no alternative if you e.g. wish to use your car, park it on-street or use the public transport. It is observed that often services start with a voluntary character but gradually develop into situation where no alternative or an alternative that is inferior or limited in options is available. As an example, consider a situation where e-ticketing is first marketed as a voluntary option of convenience for frequent users but gradually develops into a scheme where paper tickets are no longer accepted. There is a risk that data protection measures developed for the situation based on voluntary use are not, or cannot be transformed to, an adequate arrangement for mandatory use.
- Personal data processing in ITS systems often concern location data, i.e. collections of locations and associated time stamps that can (with a varying level of difficulty) be traced to an individual. Some applications only process occasional samples of location data, e.g. parking payment or local section speed control systems. Other applications by their nature collect vast amounts of location data that might in an extreme case constitute complete mobility patterns of a person or vehicle (to which a natural person can often be linked with a high probability). This can notably be the case for GNSS-based road user charging, e-ticketing in public transport, pay-as-you-drive insurance, fleet monitoring and floating cellular/vehicle data for traffic information. Such applications deserve special attention from a data protection point of view, as the potential privacy infringement resulting from unauthorised access to, or misuse of such data is considerable.

  It seems worth noting that threats related to the processing of personal mobility data are not the exclusive domain of ITS: the spectacular development in the use of GNSS- and WiFi capable mobile phones creates at least comparable issues. This area has been subject to dedicated opinions including one of the Art. 29 Working Party. Part of these recommendations could apply to ITS applications as well.
- In applications where extensive/detailed location data needs to be processed, some approaches that provide a significant improvement as to personal data protection can often be applied:
  - *Pseudonymisation*: by using short-lived identifiers the possibility of identification of individual users from the data processed can be eliminated or strongly reduced. This is particularly relevant in the context of cooperative systems.
  - *Distributed processing*: when an identification cannot be avoided, e.g. because there is a central billing process, the detailed location data may be needed to calculate the information required, but only

the aggregated results are required for the central processing. In this case, a so-called smart or thick client architecture may be applied. The On-Board Equipment or user device processes location details, but only the aggregated results are uploaded to the central system. A further improvement is realised when *Data Subject Control* is implemented: the user can inspect and delete the stored details. It is noted that a thick client approach has advantages in terms of data protection as well as communication requirements, but introduces complexity in the area of security, compliance checking, application management and appeal processes. This measure is particularly applicable in the area of Pay-as-you-Drive insurance, GNSS-based Road Pricing systems and Floating Vehicle Data. In essence, a thick-client approach also applies to eCall and the Digital Tachograph.

- *Domain separation*. The location details / usage details are labelled with identifiers that do not allow straightforward identification and are strictly shielded from the billing domain where contract ID's and person details are used. This measure is generally not as powerful as a thick client approach and does not eliminate the possibility of identification but still reduces risks.
- *Deletion / irreversible anonymisation immediately after initial processing*. Data allowing identification may immediately after (almost) real time processing, and in the equipment where the data are collected (camera or receiver), be deleted or any unique identifier may be removed. This is applicable in travel time measurements by roadside observation and in section speed control systems.
- *Data minimisation*. This is more a general requirement following from the data protection directive than a specific measure. Nevertheless it deserves mentioning that it is often possible to reduce the information that is processed based on the service options that are actually selected as compared to an approach where a superset of data is collected by default.

Privacy by Design

Developments in several areas of ITS imply ever increasing challenges to the privacy of travelling individuals. A thorough Privacy Impact Analysis (PIA) combined with a real implementation of Privacy-by-Design / Data-Protection-by-Design throughout the development process can be expected to reduce the risks to a minimum. The PIA should lead to a balanced and somehow quantified and objective outcome in terms of privacy risks. Identified high risks should lead to 'must have' requirements on the solution. The design process should start with

determining an optimum solution/architecture (multiple criteria) and set of PETs (Privacy Enhancing Technologies), that at least satisfy these requirements. For ITS applications the set of design principles/PETs listed in the previous paragraph are particularly relevant. The Privacy-by-Design process should assert that the privacy-driven requirements are elaborated and taken along in the entire development process, from global design to validation and verification. At this point, it is not clear if, how and when Privacy-by-Design / Data-Protection-by-Design will be transformed from a vision of legislators into standard practice in the engineering department.

Recommendations

The type of problems that stakeholders are faced with regarding data protection / privacy depend on their perspective. Industry and data protection supervisors are regularly at opposite sides of the table. Individual data subjects often have yet another angle. It is felt however that all stakeholders will benefit if:

- personal data protection is adequately addressed in the fundament of services and applications
- clear methods, rules and approaches to comply with are available
- new services that add efficiency, safety or comfort are not hampered by unnecessary restrictions
- data subjects feel well-informed and comfortable concerning their privacy when using new services and applications.

To realise this vision in the area of ITS, it seems that more coordination and more cooperation between stakeholders is needed. This leads to the following recommendations:

Recommendation 1.
The EC should take the initiative to prepare concrete guidance on personal data protection for specific applications and aspects of ITS. Such guidance should take the form of a Privacy Impact Assessment template for ITS applications and services. Apart from clearly describing a PIA method and procedure, it should preferably include guidance for Privacy by Design methods and criteria, PETs, security measures and codes of practice. Such generic PIA template should be complemented with tailored guidance for applications or application areas of particular concern from a personal data protection perspective. The industry and consumer organisations should be invited to participate in the development of the PIA template. The Art. 29 Working Party should be invited to provide advice, review results and finally endorse the outcome.

Recommendation 1A.
Cooperative applications would deserve a dedicated approach because of the vast amounts of geolocation data that will be processed (in the future possibly concerning all car users), the resulting potential impact on privacy, as well as the opportunity to influence such developments before their large-scale deployment.

Recommendation 1B.
Specific attention should further be paid to:

- Road User Charging on extended networks, involving passenger cars
- E-ticketing in Public transport
- Pay-as-you-drive Insurance
- Floating Vehicle Data
- Policies and mechanisms for user consent for services delivered or enabled by in-vehicle platforms, addressing issues of different drivers/passengers using a car and various applications sharing one in-car platform
- Rules, methods, tools and criteria for storage of geolocation data / mobility patterns for non-personalised purposes (e.g. traffic forecasts, urban planning, vehicle performance analysis).
- The impact of complex data protection responsibilities in ITS service chains that have multiple or joint processors and controllers.

Recommendation 2.
The EC should assert that data protection expertise is involved in standardisation working groups and the ITS R&D community as these establish the fundament and building blocks on which Privacy by Design or Privacy Enhancing Architectures are to be realised. The EC should discuss this with standardisation bodies and the ITS R&D community and should include it as a requirement when issuing mandates to CEN and ETSI for developing standards in specific ITS areas.

TABLE OF CONTENTS

1. Scope and methodology 13

1.1. Scope of action 5.1 13
1.2. Scope of this document 14
1.3. Methodology 14
1.4. Structure of this document 15
1.5. Terms and abbreviations 15

2. Literature overview and discussion 20

2.1. Legislation and case law 20
2.1.1. EUROPEAN AND MEMBER STATE LEGISLATION 20
2.1.2. PROPOSED NEW EU DATA PROTECTION REGULATION AND DIRECTIVE 23
2.1.3. CASE LAW 27
2.2. Opinions and recommendations by data protection authorities and other stakeholders 31
2.2.1. GENERIC RECOMMENDATIONS, OPINIONS, PRINCIPLES AND METHODS 31
2.2.2. GEOLOCATION SERVICES 36
2.2.3. SPECIFIC APPLICATIONS AND APPLICATION AREAS 40
2.3. Standards and standardisation 41
2.3.1. INTRODUCTION 41
2.3.2. CEN AND ISO 42
2.3.3. ETSI 44
2.4. European R&D projects 45
2.4.1. INTRODUCTION 45
2.4.2. PRECIOSA 46
2.4.3. SEVECOM 47
2.4.4. PRESERVE 48
2.4.5. EVITA 48
2.4.6. EC WORKSHOPS CONCERNING DATA PROTECTION AND ITS 49

3. Assessment of ITS applications 50

3.1. Assessment framework 50
3.1.1. BRIEF DESCRIPTION 50
3.1.2. LEGAL FRAMEWORK 50
3.1.3. LEGAL BASIS FOR THE PROCESSING 50
3.1.4. TERMINOLOGY 51
3.1.5. HIGH LEVEL APPLICATION ARCHITECTURE 51
3.1.6. TYPES OF PERSONAL DATA INVOLVED 52
3.1.7. DISCUSSION OF RECOMMENDATIONS AND OPINIONS 53
3.1.8. THREAT AREAS AND TYPES OF PRIVACY ENHANCING MEASURES 53
3.2. Individual ITS applications 54
3.2.1. DIGITAL TACHOGRAPH 54
3.2.2. ECALL 58
3.2.3. ROAD USER CHARGING 63
3.2.4. ETICKETING IN PUBLIC TRANSPORT 71
3.2.5. PARKING PAYMENT SERVICES 79
3.2.6. PAY AS YOU DRIVE INSURANCE 82
3.2.7. SECTION SPEED CONTROL 87
3.2.8. FLEET MONITORING 90
3.2.9. TRAFFIC DATA COLLECTION 94
3.2.10. COOPERATIVE SYSTEMS 103
3.3. Overview of Results 107

4. Measures and recommendations 111

4.1. Identification of areas of concern or potential improvement 111
4.1.1. ISSUES FROM THE PERSPECTIVE OF THE INDIVIDUAL 111
4.1.2. ISSUES FROM THE PERSPECTIVE OF THE PRIVATE SECTOR 111
4.1.3. ISSUES FROM A LEGISLATOR'S PERSPECTIVE 112
4.1.4. ISSUES FROM A DATA PROTECTION SUPERVISOR'S PERSPECTIVE 113
4.1.5. STATUS OF SPECIFIC GUIDANCE ON ITS 115
4.2. Relevant policy instruments of the EU 115
4.3. Analogy of smart metering in the energy sector 116
4.4. Contribution from PRESERVE project 118

4.5. iMobility Forum 118
4.6. Discussion and selection of possible measures 119
4.7. Recommendations 120

5. Conclusions 122

6. Bibliography 127

1. Scope and methodology

1.1. Scope of action 5.1

Intelligent Transport Systems (ITS) can significantly contribute to a cleaner, safer and more efficient transport system. A legal framework, the ITS Directive [63], was adopted on 7 July 2010 to accelerate the deployment of these innovative transport technologies across Europe. This Directive is an important instrument for the coordinated implementation of ITS in Europe. It aims to establish interoperable and seamless ITS services while leaving Member States the freedom to decide which systems to invest in.

The Commission already took a major step towards the deployment and use of ITS in road transport (and interfaces to the other transport modes) on 16 December 2008 by adopting an Action Plan. The Action Plan suggested a number of targeted measures and included the proposal for this Directive. The goal is to create the momentum necessary to speed up market penetration of rather mature ITS applications and services in Europe.

Under the framework contract "Technical, Legal and Organisational Support for the Implementation of the ITS Action Plan" a specific study was commissioned on Action 5.1.

ACTION 5.1	Assess the security and personal data protection aspects related to the handling of data in ITS applications and services and propose measures in full compliance with Community legislation.

In the ITS Directive 2010/40/EU, [2], Article 10 on "Rules on privacy, security and re-use of information" specifically insists on the need to ensure privacy notably by the use of anonymous data or the respect of consent in the processing of personal data. In his Opinion on the ITS Action Plan and Directive proposal [4], the European Data Protection Supervisor emphasised the need for 'privacy by design' in the development of ITS and outlined some other important issues.

The objectives and key questions of task 5.1 have been defined by the EC in the following way [1]:

The objectives of this study are to:

1. Assess the importance and impact of data protection and privacy aspects in the areas and actions of the ITS Action Plan and ITS Directive
2. Evaluate which potential measures could be undertaken and make recommendations for further action.

These objectives lead to the following key questions to be answered by the study:

1. What is the state-of-the-art concerning security and personal data protection aspects related to the handling of data in ITS applications and services in Europe?
2. In particular, which measures, rules and procedures exist or have been applied so far to deal with the data protection issues of ITS applications and services?
3. What ITS applications, or types of ITS applications, are the most subject or prone to data protection issues, or would require specific measures to address those data protection issues? Why is it so?
4. Which specific measures (legal, technical, organizational) would be required to guarantee the protection of personal data in ITS applications or services, while not prohibiting the development of novel applications and services?

1.2. Scope of this document

This document constitutes the Final Report of the study. It addresses all key questions and tasks of the study, as well as the study recommendations.

1.3. Methodology

An elaboration of the adopted methodology for the entire assignment can be found in the Inception Report, [3].

The approach for task 1 (collection and analysis of relevant documents) consisted of desk research of relevant legislation, case law, opinions and advices from

stakeholders and research and standardisation results. A number of stakeholders were invited to provide points of view, to share practical experiences and to suggest further documents of relevance.

In task 2, 10 ITS applications were analysed in more detail. The general principles of the data protection directive, [4], were applied in the context of these applications and results addressing data protection in the specific application context were discussed. The assessment framework is elaborated in more detail in 3.1.

Task 3 consisted of a workshop with ITS stakeholders from both the demand and supply side, as well as the EU and data protection authorities. Results from the workshop can be found in the workshop report, [86], and were used for the recommendations of this final report.

Task 4 consisted of the formulation of measures and recommendations, and the preparation of the final report.

1.4. Structure of this document

Section 1 – this Section – describes the scope, methodology of this study and the purpose and structure of this report.

Section 2, 'Literature Overview' reports on findings concerning legislation, rules, jurisprudence and practices relevant for data protection in ITS.

Section 3, 'Assessment of ITS applications' contains the results of the assessment of individual ITS applications.

Section 4, 'Measures and Recommendations', contains an identification and assessment of measures to improve the current situation and recommendations to that effect.

Section 5, 'Conclusions' contains the conclusions of this report.

Section 6, 'Bibliography' provides a list of referenced documents.

1.5. Terms and abbreviations

Term	Abbreviation	Definition / Explanation	Source
Article 29 Working Party	Art. 29 WP / WP29	Working party on the Protection of Individuals with regard to the Processing of Personal Data, created in compliance with Art. 29 of the data protection directive.	[4]
Automatic Number	ANPR	Software process to recognise	

Term	Abbreviation	Definition / Explanation	Source
Plate Recognition		a vehicle registration mark from a digital image containing a vehicle registration mark (number).	
Consent (of the data subject)		Any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.	[4]
Controller		The natural or legal person, public authority, agency or any 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 processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law	[4]
Event Data Recorder	EDR	Device in a vehicle that registers vehicle status information, geolocation data and driver behaviour characteristics. The data is used to analyse the circumstances in case of a crash.	
European Data Protection Supervisor	EDPS	The European Data Protection Supervisor (EDPS) is an independent supervisory authority whose primary objective is to ensure that European institutions and bodies respect the right to privacy and data protection when they process personal data and develop new policies.	

Term	Abbreviation	Definition / Explanation	Source
European Electronic Toll Service	EETS	Interoperable electronic fee collection service as defined by the interoperability directive 2004/52/EC.	Directive 2004/52/EC.
Floating Vehicle Data	FCD	Technology to calculate travel time / traffic speeds from vehicles frequently uploading location information.	
Global Navigation Satellite Systems	GNSS	System consisting of satellites and ground stations enabling a globally available and accurate positioning with a low-cost receiver. Examples of GNSS are GPS and Galileo.	
International Working Group for Data Protection inTelecommunications	IWGDPT	The Working Group founded in 1983 in the framework of the International Conference of Data Protection and Privacy Commissioners. The Group has adopted numerous recommendations aimed at improving the protection of privacy in telecommunications.	
On-Board Equipment	OBE	Equipment used in the vehicle for the purpose of one or more specific ITS services. Often used in the context of electronic fee collection and PAYD insurance.	
Organisation for Economic Co-operation and Development	OECD	International economic organisation of 34 countries founded in 1961 to stimulate economic progress and world trade. It is a forum of countries committed to democracy and the market economy, providing a platform to compare policy experiences, seek answers to common problems, identify good practices, and co-ordinate domestic and international	Wikipedia

Term	Abbreviation	Definition / Explanation	Source
		policies of its members.	
Personal data		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	[4]
Privacy by Design / Data Protection by Design	PbD	The principle of Privacy by Design states that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal.	Wikipedia
Privacy Enhancing Technology	PET	General term for a set of computer tools, applications and mechanisms which - when integrated in online services or applications, or when used in conjunction with such services or applications - allow online users to protect the privacy of their personally identifiable information (PII) provided to and handled by such services or applications.	Wikipedia
Processing (of personal data)		Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use,	[4]

Term	Abbreviation	Definition / Explanation	Source
		disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction	
Processor		A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;	[4]
Ticket Vending Machine	TVM	Machine selling (electronic) tickets or loading credits to a customer medium.	
Value Added Services	VAS	Services offered as optional add-ons to a basic (communication) service.	
Vehicle Identification Number	VIN	An unique serial number used by the automotive industry to identify individual motor vehicles, towed vehicles, motorcycles and mopeds.	ISO 3833
Vehicle Registration Mark	VRM	Unique number on a vehicle's number plate.	
Vehicle Registration Number	VRN	Synonymous to VRM.	

2. Literature overview and discussion

2.1. Legislation and case law

2.1.1. EUROPEAN AND MEMBER STATE LEGISLATION

2.1.1.1. BRIEF HISTORY

The right to privacy is a very old legal concept, but its meaning and importance strongly evolved over time with social, economical and technological developments. As Warren and Brandeis noted in 1890: 'It has been found necessary from time to time to define anew the exact nature and extent of such protection…. Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone"', [7].

In 1950, the European Convention on Human Rights and Fundamental Freedoms, [10], established a firm basis for the individual's right to privacy. From there it has found its way into the constitutions of European States.

The right to the protection of personal data as a fundamental human right was also laid down in the Treaty establishing the European Economic Community (TEC) in 1957, later converted into Art. 16 of the Treaty on the functioning of the European Union, (TFEU), [78]. Similar provisions were included in the Charter of fundamental rights in the EU, see Art. 8 [79].

The operational measures to put the right to privacy into practice were left to the individual states. However, with the development of large-scale automatic data processing systems, the need to address the treatment of personal data within such systems became apparent. The first successful attempt to harmonise privacy legislation internationally was undertaken by the Organization for Economic Cooperation and Development (OECD). This organisation issued its "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data", [6] in 1980. The fundamentals of personal data protection are laid down in this document in the form of seven principles that can be summarised as follows:

1. **Notice**: subjects whose data is being collected should be given notice of such collection.
2. **Purpose**: data collected should be used only for stated purpose(s) and for no other purposes.
3. **Consent**: personal data should not be disclosed or shared with third parties without consent from its subject(s).
4. **Security**: once collected, personal data should be kept safe and secure from potential abuse, theft, or loss.
5. **Disclosure**: subjects whose personal data is being collected should

be informed as to the party or parties collecting such data.

6. **Access**: subjects should be granted access to their personal data and allowed to correct any inaccuracies.
7. **Accountability**: subjects should be able to hold personal data collectors accountable for adhering to all seven of these principles.

The OECD Guidelines are nonbinding however. In 1981 the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was negotiated within the Council of Europe. This convention obliged the signatories to enact legislation concerning the automatic processing of personal data. This was actually taken up by several countries.

2.1.1.2. DATA PROTECTION DIRECTIVE 95/46/EC

The European Commission realised that diverging data protection legislation amongst EU member states would impede the free flow of data within the EU and subsequently proposed the Data Protection Directive, which was adopted in 1995, [4].

The data protection directive adopts and builds on the seven principles of the OECD Recommendations, [6]. Most importantly, it establishes that the processing of personal data is only allowed in case of explicit consent of the data subject (the individual concerned) or in case of a legal obligation / a major public interest.

The directive has been implemented in national laws in the EU member states. This guarantees that all main elements and requirements of personal data protection are the same across the Europe. The legal embedding in member state law differs however, as well as the exact definitions of the legal concepts (e.g. 'processor', 'recipient') applied, the notification and approval procedures and the role and competences of the national data protection supervisor. More details of the differences between member state data protection laws can be found in [8].

2.1.1.3. DIRECTIVE 2002/58/EC

The Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector can be regarded as a further more specific elaboration of 95/46/EC to address privacy issues in the area of electronic communications. It includes provisions on security of networks and services, confidentiality of communications, access to information stored on terminal equipment, processing of traffic and location data, calling line identification, public subscriber directories and unsolicited commercial communications. The Directive had to be transposed in national law by 31 October 2003 at the latest.

This Directive is relevant to ITS systems and services where they utilise data originating from electronic communications services. An example is traffic data collection using floating cellular data, see section 3.2.9.

2.1.1.4. DATA RETENTION DIRECTIVE

The Data Retention Directive amends 2002/58/EC. According to the directive, member states have to implement legislation that obliges telecom operators and internet service providers to store citizens' telecommunications data for 6 up to 24 months. Under the directive the police and security agencies will be able to request access to details such as IP address and time of use of every email, phone call and text message sent or received. A permission to access the information can be granted only through a court warrant.

2.1.1.5. ITS DIRECTIVE

The ITS Directive, [63], was adopted on 7 July 2010 to accelerate the deployment of Intelligent Transport Systems across Europe. It aims to establish interoperable and seamless ITS services while leaving Member States the freedom to decide which systems to invest in. The directive defines 4 priority areas and 6 priority actions. The priority actions are focussed on traffic and traveller information services, eCall and reservation and information services concerning safe and secure parking places for trucks and commercial vehicles.

It is explicitly recognised in the preamble of the directive that the deployment and use of ITS applications and services will entail the processing of personal data. Such processing should be carried out in accordance with Union law. In particular it is stated that the principles of purpose limitation and data minimisation should be applied to ITS applications.

Article 10 addresses rules on privacy, security and re-use of information. The article reiterates the principles of personal data protection from the data protection directive and emphasises that:

- Member states shall ensure that personal data are protected against misuse, unlawful access, alteration and loss.
- The use of anonymous data / anonymisation as one of the principles of enhancing individuals' privacy should be encouraged.
- In particular where special categories of personal data are involved, Member States shall also ensure that the provisions on consent to the processing of such personal data are respected.

As far as data protection and privacy related issues in the field of ITS applications and services deployment are concerned, the Commission should, as appropriate, further consult the European Data Protection Supervisor and request an opinion of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC.

2.1.2. PROPOSED NEW EU DATA PROTECTION REGULATION AND DIRECTIVE

2.1.2.1. INTRODUCTION

After extensive consultations on the current Directive 95/46/EC, the EC concluded that, while the objectives and principles of the current Directive are satisfactory, it has lead to a fragmentation of the implementation of personal data protection across the European Union, see [17] and [23].

The proposed new legislation therefore does not change the objectives and principles, but aims to improve the inconsistencies and inefficiencies of the current legal and procedural constellation as to data protection. The objectives of the proposed legislation are notably:

- to improve legal certainty for data controllers and citizens
- to harmonise the enforcement of personal data protection in the European Union
- to reinforce consumer confidence in online services.

The proposed new legislation consists of two elements:

- a proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), [18]. According to the Commission, this legal instrument is more appropriate than the current data protection directive. Its direct applicability "will reduce legal fragmentation and provide greater legal certainty by introducing a harmonised set of core rules"
- a proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, [19].

The *regulation* is of direct relevance to ITS applications and services. The further specification of the concept of consent, the more elaborated requirements on the information concerning the processing that has to be provided to the data subject and the role of a Privacy Impact Analysis seem of particular importance to ITS. The content of the regulation is discussed in more detail below.

It is noted that although the scope of the proposed *directive* is in the area of criminal offences, it is not entirely without relevance for ITS, as data processed in ITS applications may be claimed for the purpose of investigation or prosecution of

criminal offences[1]. It is not excluded that the design of ITS applications is occasionally influenced by anticipation of such secondary use.

It is noted that the proposed regulation and directive have not yet been adopted by the European Parliament and the Council. The content may be subject to various changes until its final adoption.

2.1.2.2. THE PROPOSED GENERAL DATA PROTECTION REGULATION

From the perspective of the targeted improvements, the changes can be classified in three categories:

1. changes that help to harmonise and reinforce personal data protection
2. changes that help to reduce administrative requirements
3. changes that facilitate the free circulation of personal data.

Category 1: harmonise and reinforce personal data protection

Compared to the items specified in Articles 10 and 11 of [4], the controller will have to provide additional information to the data subject, including:

- the storage period
- the nature of the legitimate interest pursued by the controller
- the right to lodge a complaint
- information in relation to international transfers
- information in relation to the source from which the data are originating.

The Regulation includes more specific provisions to ensure that *consent* of the data subject (regarding processing of data relating to him) is freely given, based on adequate information and given explicitly by an appropriate method ('either by a statement or by a clear affirmative action'). In addition, Article 7 of the Regulation specifies that consent "shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller".

The Regulation contains a "*right to be forgotten*" clause in its Article 17. The data subject can obtain from the controller the erasure of personal data relating to him in a number of cases, including: the data are no longer necessary for the defined purposes, the data subject withdraws his consent for the processing or the storage period consented to has expired. This right for the data subject to obtain the erasure of his personal data can be exercised at any time, whilst under the current Directive this right can be used only when the processing does not comply with its provisions. In addition, the controller who has exchanged personal data with other

[1] Currently the legal instrument covering the exchange of personal data by police and justice in criminal matters is regulated through Framework Decision 2008/977/JHA. No legal instrument exists for regulating data protection when personal data are processed by police and justice at national level. However the Council of Europe Convention 108 together with additional protocol 181 are applicable to all the Member States which are signatories to these two instruments. For further details see section 2.1.2.3.

entities shall inform these entities on the data subject's request to erase or restrict the processing.

The Regulation contains a "*right to data portability*" clause in its Article 18. Data portability is the transfer of data from one electronic processing system to and into another. To do so, the controller shall provide to the data subject his data in a structured and commonly used electronic format. With data portability, the right of access of the data subject is extended, compared with the provisions of the current Directive. It is expected to enhance data quality and to alleviate the administrative burden on the data subject.

By increasing *liability*, the Regulation reinforces the legal certainty for citizens. According to Article 24 of the Regulation, the data subject's right to compensation is extended to joint controllers and joint processors. The Regulation introduces the possibility that the processor may be held responsible and that processors and/or controllers may be jointly responsible.

The current Directive does not specify the type of *sanctions* applicable in case of infringement of the rules relating to personal data protection. It only specifies that "any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered". Article 78 of the Regulation obliges Member States to lay down rules on penalties, to sanction infringements of the Regulation, and to ensure their implementation. Moreover, administrative sanctions are significantly increased by Article 79 of the Regulation. Each supervisory authority shall sanction the administrative offences listed in Article 79 of the Regulation, imposing fines up to maximum amounts, with due regard to circumstances of each individual case.

Category 2: reduce administrative requirements

As to administrative obligations the purpose of the Regulation is to better concentrate the effort on high-risk situations and make life easier for 'ordinary' processing situations without major risks.

The Regulation removes the *notification requirements* provided by Articles 18 and 19 of the current Directive. According to the Commission, this measure will lead to annual savings for businesses of around 2.3 billion euro. A prior *authorisation* is still needed where a controller or a processor adopts contractual clauses which are not standard data protection clauses or does not provide for the appropriate safeguards in a legally binding instrument for the transfer of personal data to a third country or an international organisation

On the other hand, the controller, the processor and, if any, the controller's representative shall comply with several obligations which are not required under the current Directive. These include an obligation to demonstrate compliance, easily accessible policies with regard to the processing, availability of

documentation of all processing operations, an obligation to cooperate with the supervising authority, an obligation to report unauthorised personal data disclosure to the data subject without delay and an obligation to carry out a *privacy impact assessment* in cases where processing operations present specific risks to the rights and freedoms of data subjects.

Article 51 of the Regulation determines that controllers and processors will only have to deal with *a single national supervisory authority* in the European Union. It will be the one of the country where they have their main establishment. This measure should eliminate situations where companies that offer services in multiple countries have to deal with different legal requirements and procedures in each country where their services are offered. It is noted that this provision has been subject to criticism, in particular by the French parliament and the French supervisory authority (CNIL), which considers it to be prejudicial for citizens' rights regarding its economic, political and legal consequences, see [20].

Category 3: Free circulation of personal data

Contrary to the current Directive, the Regulation also applies to *processing of personal data outside the EU* in case:

- the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the European Union;
- the processing of personal data of data subjects residing in the European Union by a controller not established in the European Union, where the processing activities are related to:
    - the offering of goods or services to such data subjects in the European Union; or
    - the monitoring of their behaviour.

The rules for transfer of personal data to third countries are simplified as a prior authorisation is not required anymore where a transfer is based on standard data protection clauses (either standard data protection clauses adopted by the Commission or standard data protection adopted by a supervisory authority) or binding corporate rules. Note that standard data protection clauses can be adopted by the supervisory authority. Under the current Directive, these clauses can only be adopted by the Commission.

Article 45 of the Regulation provides for international co-operation mechanisms for the protection of personal data between the Commission and the supervisory authorities of third countries.

2.1.2.3. THE PROPOSED DIRECTIVE

The proposed directive, [19], is to replace the Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, often referred to as 'DPFD'.

By presenting its proposal for a Data Protection Directive, the Commission has made a policy and principle-based choice to present a new data protection instrument with a scope covering also domestic data processing operations whereas the DPFD only deals with cross-border exchange of data for police and judicial cooperation. Another element is that the included exception to the purpose limitation principle (process personal data strictly for a sharply defined purpose) is felt to be too wide. Finally, the current situation, where apart from the DFDD various sector specific legislative instruments exist (governing e.g. Interpol, Eurojust, SIS, CIS), with different data protection regimes, is regarded undesirable, see also [17]. This is changed under the new directive.

The reason to extend the scope of the DPFD is that in the view of the EC it is not feasible to distinguish domestic from cross-border data processing operations, which would be contrary to the aim to ensure efficiency and legal certainty for data processing in this area. This view is faced with opposition from several member states that claim that the subsidiarity principle is not respected by this extension. Another point of discussion is the difficulty that existing bilateral agreements between EU member states and third countries would have to be renegotiated whereas under the proposed directive, such agreements would be made by the EC, see also [22].

2.1.3. CASE LAW

From the direct search as well as inquiries to the national data protection supervisors of the EU, only few law cases were found that directly deal with personal data protection issues in ITS applications. This may be explained by the fact that the fraction of ITS in the total volume of systems and services where personal data are processed is quite small. Another reason is that privacy issues are often settled between the data protection supervisor and involved controller(s), leading to directions or advises that are consecutively adopted by the organisations. It is noted that some supervisors have authority to impose sanctions and that directions they provide may be legally binding (different arrangements in member states). Only a small fraction of data protection cases handled by supervisors is brought to a court of justice.

2.1.3.1. NATIONAL CASES

Keolis Case (France)

In the Keolis Case, [69], several users submitted a complaint to the French data protection authority CNIL concerning the anonymous transport ticket named "Korrigo" in the city of Rennes. The complaints related to the following issues:

- The anonymous ticket was far more expensive than the comparable personalised ticket (between 2.5 and 4 times)
- For the anonymous medium, only single ride tickets were offered (no season tickets / subscriptions)
- Little information on the possibility to use an anonymous ticket was provided.

The CNIL ordered that these issues were to be solved as well as other breaches of the French "Informatique et Liberté" Law (duration of the data storage, lack of information concerning users' rights, and lack of global policy concerning security and confidentiality).

The case may serve as an example and confirmation of the principle that privacy is a fundamental right of natural persons. As far as reasonably possible, anonymous use of a service shall not be positioned as premium service at higher costs or made unattractive to the customer by reduced functionality or availability.

ANPR Vialis Case (Netherlands)

In this case, [70], data collected with ANPR cameras were used as supportive evidence in a severe criminal case, showing the likely location / time / route of the suspect around the time the crime was committed. The data collected should however have been deleted from the ANPR system as there was a 'no hit' situation at the time of collection (no match with a black/grey list of vehicle registration marks), as defined by the purpose and the usage protocol of the equipment. The defendant claimed that the data would not be admissible evidence as their storage should be regarded as illegitimate. The supreme court however ruled that the – limited – privacy infringement on the personal life of the suspect does not prevail over the interest to bring justice in this particular case.

This case is an example of 'function creep', personal data are processed beyond the agreed terms and beyond their legitimate purpose. Although the outcome was likely satisfactory for most people except the suspect, it may illustrate that systems and procedures deployed in police work and criminal investigations have a risk not being subject to effective checks for compliance with applicable privacy rules and regulations.

Google Street View Case (various countries)

In France, CNIL issued a fine against Google, concerning data collection for Google's Street View application, see [71]. CNIL's enforcement committee ruled

that in collecting the WiFi data through Street View Google had committed "serious" violations of France's "Informatique et Liberté" law. Google said that it collected only "fragmentary" information. But the CNIL stated that Google recorded e-mail passwords and message content, web sites visited, as well as service set identifiers (SSID) data from WiFi networks and Media Access Control (MAC) addresses from network routers that could be used to identify and locate users.

In various other countries, the Street View data collection process of Google is or has been investigated by data protection supervisors, including Australia, Hong Kong, Canada, the US, the UK, Germany, The Netherlands and Spain; in some cases leading to directions or fines. On-going investigations include the Google Latitude application, where WiFi access point details are acquired through users of the Latitude service.

The Google cases may serve as an example of the collection of geolocation data (e.g. WiFi router MAC addresses and locations) that are to be regarded as personal data, without consent and/or adequate information to the data subjects involved.

TomTom Case (NL)

This case, [39], included an investigation by the national data protection supervisor CBP concerning the processing of off-line/historic and on-line/real-time location data of users of TomTom personal navigation devices. It resulted in a verdict that TomTom violated privacy legislation, and has to repair the situation.

The observed violation concerned the lack of sufficient information regarding the collection of historic location data and the absence of explicit consent for the processing of location data of users. Although the user is – in some cases – pointed to a privacy declaration by TomTom which states what data are collected and for what purpose, this cannot be regarded as explicit consent.

An interesting remark is made on the way that TomTom processes geolocation data: the CBP appreciates the fact that for all historical location data processing, unique identifiers are removed and a considerable effort is made to avoid the possibility to link the data to an individual. CBP however has the opinion that – e.g. by comparing the geolocation data with additional sources of data – it is still possible to link data to individuals with in some cases high probability. Therefore the data have to be regarded as personal data and explicit consent of the data subject is required.

As to aggregated historical data regarding speeds driven, which are derived from the detailed geolocation data as above and that are sold to (mainly) public authorities, CBP stated that such data were not to be considered as personal data and hence no violation of privacy law occurs.

2.1.3.2. EUROPEAN CASES

Several European cases exist that interpret the data protection directive, [4]. It is noted that none of these cases is particularly related to ITS. The aspects addressed are generally of a much wider applicability. A few major cases are briefly described below:

Rechnungshof vs Österreichischer Rundfunk and Others

In this case, see [72], the European Court ruled that articles 6(1) (c) and 7(c) and (e) of the data protection directive are directly applicable, in that they may be relied on by individuals before the national courts to oust the application of rules of national law which are contrary to those provisions.

College van burgemeester en wethouders van Rotterdam vs M.E.E. Rijkeboer

This case, lead to two important interpretations:

- Article 12(a) of the data protection directive requires Member States to ensure a right of access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed not only in respect of the present but also in respect of the past. It is to the Member States to fix a time-limit for storage of that information and to provide for access to that information which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular by way of his rights to object and to bring legal proceedings and, on the other, the burden which the obligation to store that information represents for the controller.
- Rules limiting the storage of information on the recipients or categories of recipient of personal data and on the content of the data disclosed to a period of one year and correspondingly limiting access to that information, while basic data is stored for a much longer period, do not constitute a fair balance of the interest and obligation at issue, unless it can be shown that longer storage of that information would constitute an excessive burden on the controller. It is, however, for national courts to make the required determinations.

ASNEF and FECEMD

See [74]. The court ruled that article 7(f) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as precluding national rules which, in the absence of the data subject's consent, and in order to allow such processing of that data subject's personal data as is necessary to pursue a legitimate interest of the data controller or of the third party or parties to whom those data are disclosed, require not only that the fundamental rights and freedoms of the data subject be respected, but also

that the data should appear in public sources, thereby excluding, in a categorical and generalised way, any processing of data not appearing in such sources.

2.2. Opinions and recommendations by data protection authorities and other stakeholders

2.2.1. GENERIC RECOMMENDATIONS, OPINIONS, PRINCIPLES AND METHODS

2.2.1.1. EDPS OPINION ON THE ITS DIRECTIVE AND ACTION PLAN

This document, [28], constitutes the formal response of the EDPS to the proposal for the ITS Directive and Action Plan submitted in 2009.

Part of the observations concerns the legal framework as to data protection as defined in the ITS Directive. This framework is regarded 'too broad and general to adequately address the data protection issues raised by ITS deployment in the Member States'. Without further elaboration, this could in the view of the EDPS lead to inconsistencies and fragmentation as to data protection in ITS implementation between the Member States. The EDPS points to specific elements that should be addressed in the ITS Directive.

It is observed (by the author) that part of the complexity is that in most areas the ITS Directive does not cover the actual design and deployment of ITS systems and services but addresses aspects of harmonisation and removal of obstacles for a successful introduction across borders.

The second part of the EDPS opinion addresses data protection issues that should be further addressed 'for the proper deployment of ITS'. The most important recommendations can be summarised as follows:

1. Privacy by design should be encouraged at all stages of development; in standards, best practices and specifications. In particular, the EDPS recommends the development of Best Available Technologies[2] in specific sectors and/or specific purposes in which in which the different security parameters that must be implemented throughout the lifecycle of the system would be defined in order to guarantee compliance with the EU regulatory framework.
2. An appropriate classification of the information and data to be processed through ITS should be undertaken before designing the applications and systems, in order to avoid a massive and inappropriate collection of personal data.

[2] The following definition is provided : 'Best Available Techniques shall mean the most effective and advanced stage in the development of activities and their methods of operation which indicate the practical suitability of particular techniques for providing in principle the basis for ITS applications and systems to be compliant with privacy, data protection and security requirement of the EU regulatory framework.'

3. Processing of personal data should be minimized, with regard to the entire data chain of the ITS service.
4. Many ITS applications require identity information, e.g. for billing purposes. Special measures should be taken to ensure anonymity in domains where this is possible.
5. For the purpose of interoperability, systems and databases might be connected. This requires that extra (security) provisions are made to protect against abuse of the personal data or their use beyond the agreed scope.
6. Privacy/data protection impact assessments should be conducted and Best Available Technologies should be applied in relation to particular sectors and/or purposes of use.
7. As to localization / monitoring services, the EDPS emphasizes that the use of location tools must be based on a proper legal ground, for explicit and legitimate purposes, and proportionate to the purposes to be achieved. The lawfulness of the data processing undertaken will much depend on the manner in which and the purposes for which location tools will be used. It is therefore important to clarify further the specific circumstances in which a vehicle will be tracked and its impact on the user. In any event, the use of location devices should be justified by a legitimate need and strictly limited to what is necessary for that purpose. It is important to precisely define which location data are collected, where they are stored and for how long they are kept, with whom and for which purposes they are exchanged, and to take all necessary steps to avoid any misuse or abuse of the data. Further related recommendations are provided in line with [25] and [26].
8. It is in many cases unclear what parties will act as controllers and processors in the provision of ITS services. The roles and responsibilities should be clearly specified in respect of each part of the processing.

2.2.1.2. PETS STUDY

PETs are considered vital to protect user privacy, as is stipulated in [4] and [18]. DG JUST commissioned a study to assess the economic benefits of Privacy Enhancing Technologies in 2010, [33]. Whereas the main topic is of limited relevance, the document includes a useful introduction and overview of PETs of which some are important in the area of ITS.

PETs is a complex concept that comprises a broad range of individual technologies at different levels of maturity. PETs are constantly evolving, often in response to ever more advanced threats. Data minimisation and consent mechanism are an important part of PETs. Many PETs combine various technologies, including data

protection tools and 'pure' PETs (e.g., data minimisation tools) to form integrated PET systems of varying complexity.

Several classifications of PET have been proposed, on the basis of technical or functional characteristics. The following classifications are regarded useful for this study:

The 'PET staircase', see [34], introduces 4 categories of increasing effectiveness:

- *General PET measures*: e.g. encryption, access control, role based authorisations
- *Seperation of data*: e.g. a split between the identity domain and pseudo identity domain or identity protection through a Trusted Third Party (TTP)
- *Privacy management systems*: this includes privacy rights management and tools to exercise defined privacy rules in automated processing
- *Anonymisation*: this includes non registration of personal data or immediate deletion after processing.

Another classification (Hacohen) distinguishes between Pre-usage and Usage PETs:

- Pre-usage PETs:
  - Data minimisation
  - Anonymisation
  - Limitation of Use
  - E-consent mechanisms
- Usage PETs:
  - Data quality
  - Verification
  - Encryption
  - Watermarking, tagging
  - Usage Logging.

2.2.1.3. WP29 ON THE DEFINITION OF CONSENT

The Article 29 Working Party issued an opinion on the definition of user consent in 2011, see [67]. User consent is a crucial concept in the data protection directive, [4], and the e-Privacy directive, [9]. The background of this opinion is an observed divergence of the interpretation of data subject consent across the member states, in particular when forming the legal basis for the processing of personal data. Consent is also one of the subjects on which the EC asked for input in the context of the revision of the EU data protection legal framework, see 2.1.2.

In practice, the concepts of "indication", "freely given", "specific", "unambiguous", "explicit", "informed" in relation to consent and as defined in the data protection directive, appears to leave room for different interpretations.

According to the opinion, the core issue of consent is: “If it is correctly used, consent is a tool giving the data subject control over the processing of his data. If incorrectly used, the data subject’s control becomes illusory and consent constitutes an inappropriate basis for processing.” The opinion provides examples of what should be considered a valid consent and what should be considered invalid consent. The opinion leads to the following major recommendations, formulated as suggestions for modifications to the data protection legal framework:

- “clarifying the meaning of “unambiguous” consent and explaining that only consent that is based on statements or actions to signify agreement constitutes valid consent”. The opinion points in particular at practices in the online environment where individuals often have difficulty to understand what their rights are and at what point their action has the effect of personal data being processed. As an example, internet browser settings that many users may not be aware of, may effectively imply consent to processing browsing behaviour for behavioural advertising
- “requiring data controllers to put in place mechanisms to demonstrate consent (within a general accountability obligation)”. It is noted that the type of mechanisms should depend on the context and should take into account the circumstances of the processing - in particular its risks.
- “adding an explicit requirement regarding the quality and accessibility of the information forming the basis for consent”

It is further noted that the Article 29 Working Party is not convinced that explicit consent should be the general rule for all types of processing operations. Unambiguous consent includes explicit consent, but consent from *unambiguous actions* can also be adequate depending the context. This choice gives more flexibility to data controllers the overall procedure may also be more user friendly.

2.2.1.4. E-SECURITY VULNERABILITIES IN TRANSPORT

The eSecurity WG of the e-Safety Forum published a report on Vulnerabilities in Road Transport in 2010, [29]. It consists of two parts, part 1 on so-called independent vehicle-based electronics, and the second part on interactive systems. Privacy and data protection issues are only discussed for interactive systems.

The part on interactive systems focuses on two specific applications: Road User Charging and Pay-As-You-Drive insurance.

Road User Charging

The discussion focuses on autonomous OBE based solutions, as is the foreseen basis for the EETS. A brief description of ‘thin’, ‘thick’ and ‘smart’ client concepts is provided. Thin clients forward detailed localisation data to a backoffice for calculation of the toll whereas thick clients perform such calculations in the in-

vehicle device (OBE) and only report results to the backoffice. A smart client is somewhere between these 'extreme' solutions. The forum seems to favour a thick client solution, which is considered to be a Privacy by Design driven solution, but this does not translate into a firm recommendation.

It is noted that other privacy-focused opinions in this area also lead to preference for a thick client, see [30], [31] and [32]. In general such solutions minimise the detail of personal data that are stored or processed centrally, reducing the risk of a large-scale or structural misuse of such data.

Recommendations concerning Road User Charging in this report refer to basic data protection principles from the Directive 95/46/EC.

Pay As You Drive insurance

It is emphasised in the document that a PAYD service potentially has a great impact on user privacy, as detailed data of all movements are collected. Anonymisation is regarded ineffective as quantities of localisation data kept together will allow identification of the user with relative ease and considerable probability. The application as described in this document is not supposed to collect other data than time and position (although additional data could be relevant for PAYD service).

The analysis of approaches is quite similar to the RUC case. A privacy-friendly PAYD concept is described which has close resemblance to the Thick Client solution for RUC: movement data are kept within the device and only results (premium increments) are transferred to the backoffice. Comparable to the RUC case, the device will need accurate geographical data and parameters to perform the calculations. A mechanism is therefore needed for secure (digitally signed) updates to the device, which can be sent over the air. Finally, it is mentioned that a mechanism (e.g. through a USB stick) should be provided through which the user may inspect the details on which calculations are based and which is not available for the controller/processor.

The report specifically refers to the PriPAYD concept as elaborated by the COSIC department of KU Leuven, see [82]. This is in fact an example of a Thick Client solution: all computations transforming the GPS data into billing data are performed in the vehicle's black box. The data involved in the calculation of the final premium are the number of kilometres travelled, the hour of the day, the road the user has chosen, and the rate per kilometre given by the insurer. To perform the conversion, maps have to be available to the black box, and calculations have to be performed to match the coordinates with road types. The rates imposed by the insurer or other policy parameters can be initialised in the black box when installing it, and they (as well as the geographical data) can be updated later in a trustworthy manner through signed updates.

2.2.2. GEOLOCATION SERVICES

2.2.2.1. WP29 OPINION ON LOCATION DATA FOR VAS

The Art. 29 WP adopted its opinion on location data for Value Added Services in 2005, [26]. It is noted that since that time, a strong development has taken place in this area both concerning functional and technical capabilities and the use of location-based services. Relevant additions that reflect some of these developments can be found in the more recent Art. WP29 Opinion on geo-location services, [25].

The document on VAS observes that location-based services no longer exclusively locate people on their own request but include applications where they are being located on the request of a third party. It is noted that people can be located by their mobile phones even if they are not using them (provided they are connected to a network). It is stated that the two applicable directives, [9] and [4], provide a stable basis for data protection in this area, yet some elements deserve specific attention:

- In view of the very sensitive nature of the processing of location data, the Working Party would draw the attention of service providers to the need to provide clear, complete and comprehensive information on the features of the service proposed.
- Where information is provided in the general terms and conditions for the service, the Working Party recommends that the service provider should give the individuals concerned the opportunity to consult the information again at any time and by a simple method, such as via a website or while using the service
- Consent by the data subject should be specific and explicit: this explicitly rules out consent being given as part of accepting the general terms and conditions for the electronic communications service offered.
- Offering a service that requires the automatic location of an individual (e.g. the possibility of calling a specific number to obtain information on the weather conditions at one's location) is acceptable provided that users are given full information in advance about the processing of their location data.

The Working Party stresses that the use of location data is to be provided with adequate safeguards, including:

- a value-added service based on location data may be provided either directly by the electronic communications operator or via a third party. In any event, effective measures are needed to verify and authenticate requests for access to location data made by third parties offering a value-added service.
- an end-user terminal could also provide a high degree of protection with its own built-in location capability. The location data can then be

processed by an Identity Management System to deliver pseudonyms to multiple service providers.

- providers of value-added services must take appropriate measures when obtaining consent to ensure that the person to whom the location data relate is the same as the person who has given consent. Where the processing of location data is ongoing (e.g. services such as Find-a-friend), the service provider must confirm subscription to the service by sending a message to the user's terminal equipment after consent has been received, and if necessary, request confirmation of the subscription
- the option to withdraw consent has to be offered in a user-friendly way.

2.2.2.2. WP29 OPINION ON GEO-LOCATION SERVICES ON SMART MOBILE DEVICES

The Working Party observes that fascinating new uses of smartphones imply new privacy risks. People keep their mobile devices close to themselves all the time. The device is hardly ever turned off. This allows providers of geolocation services to build a detailed pattern of mobility and activity, which may also include special (sensitive) categories of information, e.g. visits to hospital, places of worship, presence at a demonstration etc. Monitoring of devices can be done secretively or semi-secretively when people forget or are not explicitly informed that a location service is switched on or when accessibility settings are switched from private to public. As with other new technology, a major risk with the use of location data is function creep, the fact that based on the availability of a new type of data, new purposes are being developed that were not anticipated at the time of the original collection of the data. With the help of geolocation technologies smart mobile devices can be tracked for purposes ranging from behavioral advertising to monitoring of children.

Because location data from smart mobile devices reveal intimate details about the private life of their users, the main applicable legitimate ground is prior informed consent. Consent cannot be obtained through general terms and conditions; rather, consent must be specific and explicit for the different purposes that location data is collected, used or otherwise processed (e.g., profiling or behavioral targeting).

It is noted that a unique identifier, in the context of geo-location services, allows the tracking of a user of a specific device and, thus, enables the user to be “singled out” even if his/her real name is not known. This indirect identiability applies to WiFi access points as well. The MAC address of a WiFi access point, in combination with its calculated location, is inextricably linked to the location of the owner of the access point. A reasonably equipped controller may calculate an increasingly precise location of a WiFi-access point based on the signal strength and of the ongoing updates of the location through the users of its geolocation service.

In the area of geolocation services on smart mobile devices, specific recommendations of the Working Party to comply with the data protection directive include:

- Verify that the consent is specific, informed and explicit. The consent for certain applications to use location data may be otherwise be invalid because the information about the key elements of the processing is incomprehensible to the user, outdated or otherwise inadequate.
  - Users must be provided with notice of the collection which is accurate, clear and understandable for a non-technical audience of the collection, use or other processing of geolocation data. This notice must be permanently and easily accessible.
  - An opt-out mechanism does not constitute an adequate mechanism to obtain informed user consent.
  - The consent should be limited in time; users should be asked for consent at least once a year
  - Users must be able to withdraw their consent in a very easy way, without any negative consequences for the use of their device
  - If purposes of processing change in a material way, renewed consent of the data subject is required.
- By default, location services must be switched off.
- With respect to *employees*, employers may only adopt such technology when it is demonstrably necessary for a legitimate business purpose and the same purpose cannot be achieved with less intrusive means.
- With respect to *children*, parents must judge whether the use of location data is justified in specific circumstances.
- Users have the right to access their location data in a human-readable format and to rectify and erase the data. They also have the right to access, rectify and erase *profiles* compiled based on their geolocation data. The Working Party recommends (secure) online access to these data by the data subject.
- If the developer of the device's operating system or a data controller of the geolocation infrastructure processes a unique number such as a MAC address or a UDID in relation to location data, the unique identification number may only be stored for a maximum period of 24 hours, for operational purposes.

2.2.2.3. IWGDPT COMMON POSITION ON LOCATION INFORMATION

It is noted that this paper of the International Working Group on Data Protection in Telecommunications, the 'IWGDPT position on privacy and location information in mobile communication services', [27], dates back to 2004. It was published against the background of increased positioning capability and accuracy becoming available in mobile networks as well as GPS becoming more widely available in handhelds and other personal devices. The scope of the paper concerns Value

Added Services, where it is assumed that location information either originates from the network operated by mobile operators or in the device itself. It is stated that the position information created in the device is easier the control than information originating from the network. It should be noted that the massive deployment of location based services through smartphones did not yet take place and some of today's possibilities and resulting new privacy issues could not yet be foreseen. Nevertheless, the 9 principles that are to be observed do not seem to have lost their validity.

The recommendations of specific relevance for this study are listed below (clustered summarized):

1. Precise location information should not be collected as a standard service but only if needed for a specific service the user wishes to use.
2. The mobile subscriber should always be able to control both the possibility of using any location services or specific location services. The provider should give the subscriber the opportunity to opt-in to the possibility of the use of any location services when presenting the subscriber contract. The subscriber may opt-in at this point or at any future time and may opt-out of all location services at any time.
3. When the telco provides position information to third parties, the informed consent of the user is essential. The user should also be able to specify the precision/granularity of the position information involved. The consent may relate to a continuous service but can also be restricted to a single transaction.
4. The creation of individual movement profiles is not allowed, unless for a specific service to which the user has given is informed and unambiguous consent.
5. Wherever possible, mobile network operators should not communicate location information together with personally identifiable information but use pseudonyms instead.
6. Location information should be erased when no longer needed for the provision of the service.

2.2.2.4. Opinion of the Information Commissionner of Ontario on WiFi Positioning systems

The information commissioner of Ontario published a paper on the privacy threats relating to the use of Wi-Fi in mobile devices in 2011. It carries the alarming title: "Wi-Fi Positioning Systems: Beware of Unintended Consequences - Issues Involving the Unforeseen Uses of Pre-existing Architecture", see [68]. Although this opinion is not specifically targeting ITS, the issues and recommendations have quite some relevance to ITS. In the first place it is observed that handhelds are

becoming one of the major user front ends for ITS applications. Dynamic information on public transport services, e-ticketing, navigation and parking information and payment services are often delivered using such platforms. In the second place, the fundamental privacy issues identified for WiFi, may serve as a lesson from which the development of vehicular ad-hoc networks (as needed for cooperative applications) can benefit.

In this paper it is observed that handhelds/smartphones are becoming more and more crucial in the daily lives of a majority of people, carrying and using the device almost everywhere and without ever turning it off. Whenever an individual uses location-based services on his or her mobile device, an unique identifier of nearby traceable Wi-Fi access points called a Media Access Control (MAC) address is relayed. This location information may be compiled into a profile of an individual over time, such as where they have travelled to, shopped, eaten or banked. “In addition, potential unintended consequences stem from the intrinsic nature of MAC addresses that are at the core of current networked communications. For instance, with minimal time and resources, one may be able to associate MAC addresses of mobile devices to physical addresses, and then to a specific individual. Furthermore, depending on future developments, it may even be possible that individuals using geolocation services could inadvertently report the MAC address (and, simultaneously, location) of mobile devices belonging to friends, family or co-workers - creating an unintended 'unknowing informant' model of data collection."

The authors of the paper warn that when designing an architecture the question of unintended uses, inadvertently introduced through the existence of that architecture, should form part of a privacy threat risk analysis. In no case, should the MAC address of end-user devices be collected or tracked without the consent of the owners of such devices.

It is noted (by the authors of this study) that this advice seems very sensible but is a bit late to influence the design and protocols of general-purpose WiFi networks that have already been deployed on a massive scale around the globe. It seems however that the lessons learned are taken very seriously in the on-going development of automotive ad-hoc networks, see 2.3.3.

2.2.3. SPECIFIC APPLICATIONS AND APPLICATION AREAS

A number of opinions and guidelines concerning specific ITS applications or ITS application areas have been published by the EDPS, the Art. 29 WP, the IWGDPT and some national data protection supervisors.

To avoid duplication of information, documents concerning the 10 selected ITS applications are discussed in the respective subsections of Section 3.

2.2.3.1. *IWGDPT WORKING PAPER ON EVENT DATA RECORDERS IN VEHICLES*

The IWGDPT published a paper on the use of event data recorders in 2012, see [80]. In this document event data recorders (EDRs) are defined as devices that record data from vehicle sensors and in principle keep such data only concerning a limited timeframe before, during and after a vehicle crash.

The processed data do not only relate to the technical status of a vehicle but also to the behaviour of the driver (e.g. brake oil pressure, speed, safety belt usage and sometimes video data). It is noted in the working paper that EDRs are increasingly being linked to communication systems that will transmit data in case of a crash (see eCall). It is further noted that the EDR can technically have multiple secondary uses for a range of stakeholders (police, employers, vehicle manufacturers), which requires careful consideration of personal data protection aspects.

In view of the above the IWGDPT recommends that:

- *Legislative framework*: an appropriate legislative framework for EDR is set forth or clarified
- *Transparency*: processing by EDRs shall be completely transparent. This would relate both to manufacturers (making the user/owner aware what data processing takes place in the vehicle by the EDR) as well as data controllers for the applicable specific services (e.g. employers, insurers, car rental companies).
- *Owner's consent*: as a rule the owner's explicit and informed consent should form the legal basis, and this should be based on 'opt-in'. Mandatory installation for any purpose would require a specific legal basis.
- *Data Minimisation*: data processing shall not be excessive and anonymous/anonymised data should be used whenever possible.
- *Privacy by Design*: should be applied for the entire system/service.
- *User Access*: tools and procedures should be in place to provide the data subject with free and full access to his/her data.
- *Data security and integrity*: measures should be in place to prevent unlawful access, alteration or loss of data.
- *Employee monitoring*: the employer should take into full account relevant legislation when installing devices capable of processing geolocation or driver behaviour related data.

2.3. Standards and standardisation

2.3.1. INTRODUCTION

Standards are by their nature intended for use in multiple and often different implementations. A standard or even a set of standards will therefore hardly ever

cover a real-life implementation in all its aspects, but only specific characteristics, components or interfaces.

As to privacy and data protection, the approach taken in a certain implementation always depends on e.g. the purpose of processing, the nature of information processed, details of the manual and automated processes and the data subjects involved and a certain business and political context. It is therefore unrealistic to expect that standards will ever serve as a set of instructions how to realise adequate protection of personal data in a specific situation.

On the other hand, it is widely recognised that certain technical measures taken on the level of 'building blocks', i.e. components and interfaces, may strongly facilitate adequate protection in the systems using them and may be part of a 'privacy by design / data protection by design' approach. Incorporating such measures in a (formal) standard usually has the great advantage of significant cost reduction and an increase in the quality of implementation. This advantage increases if the building blocks have a wider applicability in terms of functions or applications for which they can be used. Of course, a wider applicability risks being inadequate in a specific situation. This implies a trade-off which is to be made on a case to case basis.

Next to technical standards, standards that describe approaches or frameworks for data security can be valuable. Such standards generally do not prescribe what measures are to be taken or how they are to be implemented in detail, but provide guidance on an approach that should help to realise adequate security / data protection.

2.3.2. CEN AND ISO

2.3.2.1. ISO

It may be justified to note that optimum provisions for data protection are not always on the top of the minds of all (industry) experts involved in elaborating standards. The ISO/TMB/PSC was installed to address this issue, which resulted in a set of recommendations to the ISO/TMB which were adopted in February 2012, [11]. The recommendations include measures for creating awareness as to privacy rules and regulations, instructions on how to deal with privacy during development of standards for applications which are capable and intended to collect personal information, and specific new work items to be undertaken with a primary focus on privacy:

1. a generic Privacy Impact Assessment standard
2. a Privacy Management System standard including vocabulary, requirements, a code of practice etc. – more or less comparable to the EN 27000 series on security.

3. a guideline on data deletion
4. standards for privacy seal programs aiming at a mutual recognition of the level of personal data protection offered.

The recommendations also include distribution of privacy related standards at zero cost.

As to point 2. above : this work has already started and the first part, ISO/IEC 29100 is available, [12]. It provides a privacy framework which - specifies a common privacy terminology; defines the actors and their roles in processing personally identifiable information (PII); describes privacy safeguarding considerations; and provides references to known privacy principles for information technology. EN 29101 (under preparation) will address the privacy reference architecture.

ISO/TR 12859:2009 gives general guidelines to developers of intelligent transport systems (ITS) standards and systems on data privacy aspects and associated legislative requirements for the development and revision of ITS standards and systems.

The ISO 27000 family of standards provides a generic framework for information security management that enables an overarching and systematic control of an organisation's information security risks including identification and classification of threats and vulnerabilities, defining appropriate controls and monitoring that the information security controls continue to meet the organization's information security needs on an ongoing basis, [15][16]. It is noted that these standards are not specific for personal data protection, but personal data protection can be easily integrated in the overall information security management process.

A considerable number of ISO (as well as IEEE, NIST, FIPS, IETF, ITU) standards concern frameworks, requirements, methods, protocols and algorithms for information security. Obviously, these techniques are relevant for personal data protection. A more detailed assessment of generic information security standards is not relevant for scope of this study.

2.3.2.2. CEN

Within CEN/TC278 a work item was recently adopted to prepare a Technical Report *'Privacy aspects in ITS standards and systems in Europe'* as a guide for the working groups how to deal with personal information and data in standards and technical reports.

CEN CWA 16113:2010 provides a set of Personal Data Protection Good Practices agreed between expert participants at a CEN workshop with the same denominator. It mainly highlights and summarizes the legal obligations as to

privacy, and provides some practical guidelines to the industry on how these can be fulfilled in the most effective and efficient way, [13].

2.3.3. ETSI

In the relatively new area of cooperative applications, coordination between ETSI and CEN is established to avoid work overlap and inconsistencies of results. ETSI deals with physical characteristics, protocols and basic messages of V2V and V2I communication whereas CEN has an application focus. ETSI TC ITS liaises with CEN TC278/WG16. ETSI TC ITS also cooperates closely with the Car to Car Consortium (CCC).

TC ITS focuses on a basic set of applications that are deemed deployable in a first step after completion of the standards. Specifically addressed applications are cooperative awareness, longitudinal collision risk warning and intersection risk warning. Work in TC ITS further concentrates on a facilities layer that is generic for all applications. It includes communication management, service announcement, local dynamic map and specifications for location and time information used in messages.

A subgroup of TC ITS, WG5, deals with security and privacy aspects. The status of relevant documents of WG5 can be found in Table 1 below.

Table 1 Overview of ETSI TC ITS security and privacy related standards/reports

ETSI Reference	*Name*	*Approval status*
TR 102 893	Threat Vulnerability and Risk Analysis	Published
TS 102731	Security Architecture	Published
TS 102867	Security mapping IEEE 1909.2	Approved
ES 202910	ITS station security management	In draft pending approval by WG5 in April 2012
TS102943	Confidentially Services	WG5 approved pending TC ITS approval
TS 102941	Identity, trust and privacy	WG5 approved pending TC ITS approval
TS 102942	Access Control, secure and privacy-preserving services	WG5 approved pending TC ITS approval
TS 102940	Security architecture and management	WG5 approved pending TC ITS approval

Two message sets have been defined that are considered to be building blocks for cooperative safety and traffic management applications:

- The Cooperative Awareness Basic Service (CAM). This can be regarded as a 'heartbeat message' from vehicles and roadside periodically (every 0,1 s) broadcasting safety-relevant status information.
- The Decentralised Environmental Notification Basic Service (DENM). This is an event-triggered message announcing a detected road hazard.

It should be noted that the CAM messages can be picked up by any receiver within the communication range (several 100s of meters). Some form of identification is required in these messages in order to be able to link status (location, speed) information to a particular vehicle over time for an assessment of potential safety hazards. For safety reasons it is also of major importance that effective authenticity and integrity measures are provided. And finally, the traceability of individual vehicles is to be reduced to a minimum for privacy reasons. These partly conflicting requirements have lead to an approach using digital signatures based on short-lived public key certificates. This is in fact an approach of pseudo-identities: the processing of personal data cannot be completely avoided, but the amount of mobility data that can be linked to a specific vehicle is normally limited to a time window of a few minutes.

In general, cooperative applications impose great challenges in the area of security and privacy:

- As safety is at stake, trust in the identity of communicating entities and the correctness of information is crucial.
- A centrally organised trust scheme is not adequate for vehicle ad-hoc networks.
- Given the nature of the applications, time windows for communication are very short and any overhead for key establishment, encipherment or signing can only a fraction of the time budget.
- An approach where vehicles periodically broadcast messages including an identity, is potentially vulnerable to tracking by unauthorised entities.

It is further noted that a technically and economically viable solution to generate/revoke key pairs and certificates on such a massive and dynamic scale is not obvious. This seems an issue which still stands in the way of large-scale deployment.

2.4. European R&D projects

2.4.1. INTRODUCTION

In the last decade a number of projects were funded under the EC FP6 and FP7 framework that relate to the security and privacy issues in ITS. The ones with most relevance to this study are briefly described in this subsection.

2.4.2. PRECIOSA

The PRECIOSA (Privacy Enabled Capability In Cooperative Systems and Safety Applications) is an FP7 STREP project focussed on privacy issues in the area of cooperative systems which was concluded in 2010. An important part of the work was dedicated to elaborating Privacy by Design in a form that is appropriate for the disciplines that are actually involved in designing ITS. So far, the concept of PbD has been almost exclusively discussed on a legal level at a galactic distance from the development departments of the industry. The PRECIOSA Guidelines, [54], provide a number of interesting suggestions to improve the ITS development process from a privacy point of view. The – in our view – most important recommendations are summarized below:

- *Privacy by Design process*. The traditional waterfall model of system development (or alternatives) should be complemented with a 3-stage PbD process consisting of a privacy requirements analysis stage (Stage I), a privacy-aware design and implementation stage (Stage II) and a privacy verification and assurance stage (Stage III). Stage I includes the specification of a minimised set of data, the specification of data policies and a trade-off leading to a decision on PETs that will be applied. It is noted that many technical and procedural issues have to be solved when implementing a PbD process in practice.
- *A runtime architecture enforcing data protection policies*. A so-called Privacy-enforcing Runtime Architecture (PeRA) should be applied which safeguards that defined strict rules derived from privacy policies on e.g. data exchanges are respected on the level of software components in ITS systems. This can be considered a specific 'usage PET', see 2.2.1.2. Details of this architecture can be found in [66].
- *User consent approach*. The current model of 'notice and choice' in which the user is confronted with often complex statements on privacy policy or options when using a service and asked to tick boxes does not seem effective. It should be replaced by a 'rules-and-tools' model. Rules could be government regulations that limit how personal information can be used, or generic personal choices on what information can be provided in what contexts. Tools would e.g. be digital reminders, such as an on-screen alert that enhance user perception that an action has privacy implications.
- *Bridging the gap between legal/policy domain and the development domain*. To adequately implement privacy criteria of different stakeholders, high level privacy criteria (described in the language of stakeholders as data subject and data controller) must be translated into technical requirements which can be analysed and implemented by formal methods and tools such as PETs. Currently, the process of translating high level requirements (such as the results of a Privacy

Impact Assessment) into technical requirements is poorly understood. There exist several challenges to translate descriptions from one language into another because the languages address different purposes and thus have different techniques of expression and focus on different aspects. While performing translation process, details of the original description are often lost. Such effects must be taken into consideration with the guarantee that they do not affect the intended purposes. To address these challenges, promising approaches exist to create a shared understanding of the privacy domain by creating standard definitions in form of models and ontologies. We may use these standards to extend the existing analyses by integrating requirement engineering mechanisms, best practices, design patterns, and other well-understood techniques.

It is noted that key PRECIOSA results actually have a broader applicability than cooperative systems and would be applicable beyond ITS.

2.4.3. SEVECOM

SeVeCom (Secure Vehicular Communication) is a finalised EU-funded project that was executed from 2006 to 2009 and targeted on providing a full definition and implementation of security requirements for vehicular communications in a cooperative context. Sevecom addressed the security of the future vehicle communication networks, including both the security and privacy of inter-vehicular communication and of the vehicle-infrastructure communication.

Main results in terms of security architecture and security mechanisms are reported in D2.1, see [65]. Important topics addressed / elaborated are:

- *Key and identity management*. The contribution specifically addresses the problem of public key certificate management/revocation in a context of massive numbers of short-lived identities distributed over large numbers of cars with gaps in connectivity.
- *Security Architecture*: An architecture consisting of 5 security modules including a privacy management module which leverages on pseudonyms to offer a certain level of privacy in vehicular ad-hoc networks. The privacy management module has a pseudonym component that generates, stores and refills pseudonyms and a pseudonym application component that decides when to change pseudonyms. An identity and trust module provides and manages identities and certificates of all entities directly involved in vehicular communications, i.e. vehicles and roadside units. It has a component for Identity Management to manages the long-term identifier, and certificates containing vehicular attributes. The Trust Management

component describes the backend infrastructure (e.g. a PKI) that provides public key registration, certification, and revocation services.

- *Secure communications.* Message formats for different types of interactions in V2V and V2I communications.

The results of SEVECOM were input to the current standardisation efforts in ETSI TC ITS and CEN/TC278/WG16.

2.4.4. PRESERVE

PRESERVE is an on-going FP7 funded research project dedicated to addressing and demonstrating security solutions for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications. It builds on the results of SEVECOM. PRESERVE will develop an integrated V2X Security Architecture (VSA) and demonstrate a close-to-market implementation termed V2X Security Subsystem (VSS). This VSS will provide a sophisticated security system for use in V2X communication systems that can be used in other Field Operational Test projects.

Central part of this VSS will be a Hardware Security Module (HSM) which provides extra protection to secret key material. Additionally, the HSM will be used as cryptographic execution accelerator – especially speeding-up the Elliptic Curve (EC) signature verification.

So far – as this project is still on-going - only D1.1 has been published, see [64]. It presents a homogenized view of relevant literature, enriched by the knowledge and experiences from the ETSI standardization process and other automotive activities (e.g., the Car-to-Car Communication Consortium).

2.4.5. EVITA

EVITA is an EU FP7-funded project which was concluded in 2011. It focused on secure and trustworthy *intra-vehicular communication* as the basis for trustworthy communication among cars or between cars and the infrastructure (i.e. cooperative applications, V2V and V2I). The objective of the EVITA project is to design, verify, and prototype an architecture for automotive on-board networks where security-relevant components are protected against tampering and sensitive data are protected against compromise when transferred inside a vehicle. By focusing on the protection of the intra-vehicle communication EVITA complemented other e-safety related projects that focus on the protection of the vehicle-to-X communication, including measures to prevent eavesdropping on V2I/V2V messages.

EVITA's deliverable D2.4, [84], addresses privacy and liability issues. It concludes that, in case the use of the on-board network is not regulated by specific legislation (as – possibly – for use cases such as eCall or road toll pricing), the introduction of the service will not be possible without the informed consent of the data subject.

The document further concludes that:

- "At the design stage of each specific service it will be necessary to establish how the data subject can best be informed and how his/her consent can be collected. This will not be simple in all cases because designers will certainly need to solve specific practical questions such as how to include occasional drivers, etc. A particularly difficult problem in this context is the attribution of the roles of controller and processor or, in other words, how to fit these traditional concepts of Directive 95/46/EC in complex ITS processes involving multiple actors."
- "Since communications between vehicles and between vehicles and infrastructures will occur on publicly available networks, Directive 2002/58/EC comes into play as well. Questions such as the applicability of the mandatory security breach notification to users and public authorities, or how to implement the requirement to collect the prior consent of the user before storing information and gaining of access to information that is already stored in the on-board equipment, can only be solved in the context of every specific use case."
- Providing a series of building blocks to enhance the privacy and the protection of personal data in the context of automotive on-board networks, EVITA is essentially a contribution to what is generally called “privacy by design”.

2.4.6. EC WORKSHOPS CONCERNING DATA PROTECTION AND ITS

In the past 5 years a number of dedicated workshops on the theme of privacy in ITS applications were organised by the EC, notably:

- In-vehicle Telematics and Co-operative systems workshop on privacy and data protection issues, 13 Feb 2007[3].
- In-vehicle Communication, Telematics and Co-operative Systems Workshop on Security and Privacy Issues, eSafetySupport, 27 May 2008, European Commission[4].

[3] Agenda and presentations can be found on: http://ec.europa.eu/information_society/activities/esafety/before/2007/index_en.htm

[4] Agenda and presentations can be retrieved from http://www.esafetysupport.org/en/esafety_activities/esafety_working_groups/esecurity/esecurity_workshop_02.htm

3. Assessment of ITS applications

3.1. Assessment framework

This subsection provides a basis for the analysis of privacy aspects for specific ITS applications in the next subsection. Each application will be described in a common structure which is clarified in the subsections below.

3.1.1. BRIEF DESCRIPTION

This subsection serves as a brief introduction to, and demarcation of the application discussed.

3.1.2. LEGAL FRAMEWORK

In general, the applicable legislative framework as to data protection is the EU data protection directive, [4]. Personal data processed for the purpose of providing electronic communication services are bound to the specific regime of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector [9]. As this is the case for all ITS applications, it will not be repeated in the specific elaboration of applications in the next subsection.

In cases where specific regulations apply that significantly deviate from the generic directives mentioned above, a specific remark is made under this subsection.

3.1.3. LEGAL BASIS FOR THE PROCESSING

This subsection is to describe the legal basis that applies to the specific ITS application (area). In general, the legal basis for the processing of personal data in ITS applications is the data protection directive [4]. The following classification is used to describe the legal basis in relation to [4]:

- LB1: processing is necessary for compliance with a legal obligation originating from national or EU legislation (Art. 7, clause c)
- LB2: the data subject has given explicit consent for the processing of his personal data, mostly in the context of using of a voluntary service (Art. 7, clause a)
- LB3: processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1), (Art. 7 clause f).

The data protection directive lists three other grounds on which processing of personal data may be legitimate. These grounds are generally not relevant in the

context of ITS applications and do not appear in the assessment of applications in this Section.

For some applications, the legal basis may differ between deployments. An example is an electronic toll service which can either be a voluntary service for those who do not wish to pay manually, or a legal obligation when no manual alternative exists to pay the toll.

3.1.4. TERMINOLOGY

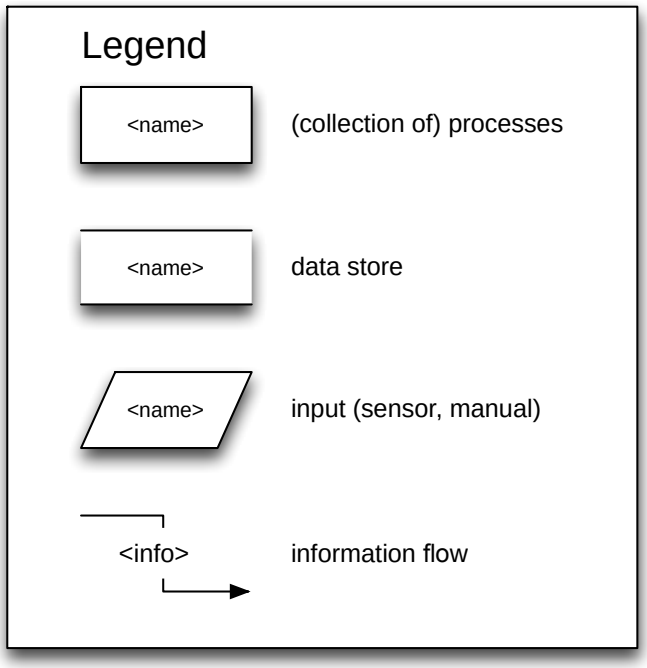
The following generic terms are used to discuss the applications from a privacy point of view.

- *Data subject*: identified natural person, or natural person that can be identified.
- *Personal data*: information relating to a data subject.
- *Filing system*: any structured set of personal data accessible according to specific criteria.
- *Controller*: entity responsible for the processing of personal data, determining the purposes, conditions and means.
- *Processor*: entity that processes personal data on behalf of a controller.
- *Data subject's consent*: any freely given specific, informed and explicit indication of the data subject that he agrees that his personal data are processed.

Where needed, additional application-specific terms will be introduced.

3.1.5. HIGH LEVEL APPLICATION ARCHITECTURE

This subsection describes the high-level (information) architecture of an application, as far as relevant for privacy. It describes the main components of the system and the most important information that is exchanged between them from a personal data protection point of view. The following symbols are used in the diagrams:



It is noted that different architecture solutions may exist for an application. The description will focus on the common characteristics. When of specific importance, alternatives will be presented.

3.1.6. TYPES OF PERSONAL DATA INVOLVED

This subsection addresses the character of personal data involved, which will also indicate the potential sensitivity. According to the data protection directive, categories of specific sensitivity are “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life”. In ITS services such data are normally not processed. Location or mobility data that are often processed in ITS services are not listed among most sensitive categories. Most people will find such data in the hands of unauthorised entities far from harmless however. It is also rather obvious that the sensitivity increases with the amount/completeness (e.g. a complete GPS log of locations and timestamps versus an occasional single registration of a vehicle at a specific location) and the resolution (time, location) of the data. It is also noted that detailed location data may reveal information that would qualify as sensitive data. As an example, location data may reveal regular visits to a certain church or hospital, in which case the location data themselves have to be regarded as sensitive data. This is to be assessed on a case-by-case basis. It is clear however that such risks are higher if geolocation data are more detailed and/or more complete.

To assess the differences between ITS applications in terms of the sensitivity of data that are processed, we therefore use the following rudimentary categories:

- Category A: location data
  - A1: Occasional single samples of position and time
  - A2: Connected samples that allow reconstruction of trips/routes, but scattered, incomplete in terms of geography or time.
  - A3: Complete traces of a vehicle or person
- Category B: trip data without location information, e.g. distance and time
  - B1: Occasional samples
  - B2: (Almost) Complete logs of all movements
- C: Details of driving behaviour (e.g. speed, acceleration, brake power applied, driving hours)
  - C*: Driving behaviour that may indicate a health status (e.g. occurrence of an accident) or a criminal offence (e.g. excessive speeding) have a special status and should be regarded as 'sensitive data' in terms of the data protection directive. It is noted that in some countries and certain data protection authorities (e.g. the CNIL) the processing of data relating to an offence/crime is not permitted at all (except for criminal prosecution, national security and other purposes that are outside the scope of the data protection directive).

3.1.7. DISCUSSION OF RECOMMENDATIONS AND OPINIONS

For each application described, this subsection provides a discussion of privacy/data protection issues in an application area based on specific inputs identified. It includes the recommendations and opinions that have been published on the specific application by data protection supervisors and other stakeholders.

3.1.8. THREAT AREAS AND TYPES OF PRIVACY ENHANCING MEASURES

In the 'threats and risks' subsection main types of threats are identified that can be considered typical for an application. Three generic threat types will be assessed:

- T1: Unauthorised access to personal data, by eavesdropping, unauthorised actions of staff, hacking etc.
- T2: Re-use of personal data beyond the legally defined purpose or beyond the scope of the consent of the data subject.
- T3: Excessive processing, i.e. processing more personal data than required for the purpose.

It is emphasised that this does not imply that the indicated categories always pinpoint residual risks in a particular scheme, as this largely depends on the way the system is designed and operated and the countermeasures that are taken.

The following set of general privacy enhancing measures is used to characterise elements of the recommendations and current practices discussed in the previous subsection:

- M1: anonymisation
- M2: pseudonymisation
- M3: data minimisation
- M4: domain separation
- M5: user consent mechanisms
- M6: deletion immediately after initial processing
- M7: distributed processing
- M8: data subject control

3.2. Individual ITS applications

3.2.1. DIGITAL TACHOGRAPH

3.2.1.1. BRIEF DESCRIPTION

The tachograph is a device that records the driving time, breaks, rest periods as well as periods of other work undertaken by a driver. This is aimed at helping to enforce the rules on driving times and rest periods and monitor the driving times of professional drivers in order to prevent fatigue, and guarantee fair competition and road safety. Since 2006, tachographs in new vehicles are to be digital, which allows a more secure and accurate recording and storage of data than the previous analogue tachograph. This device records all the vehicle's activities, for example distance, speed and driving times and rest periods of the driver. The system includes a printer for use in roadside inspections and the driver has a card incorporating a microchip, which the driver must insert into the tachograph when taking control of the vehicle. The driver card is the second recording unit, drivers frequently changing vehicle carry their activity records on a single chipcard. Different types of cards are used for workshops and inspectors. It is obligatory to install a digital tachograph in new vehicles having a mass of more than 3,5 tonnes (in goods transport) and carrying more than 9 persons including the driver (in passenger transport).

A major amendment to the current regulation has been proposed recently that affects the technical capability of the equipment, see [37]. The main modifications proposed are the following:

- A DSRC-based wireless interface for control purposes, which can be used in free-flow traffic. This would considerably enhance the effectiveness and efficiency of enforcement. It would also reduce the administrative burden on the enterprises.
- Inclusion of a GNSS sensor for positioning. It is foreseen that only start and end location of daily use of the vehicle are logged.

- An ITS-interface, either wired or wireless, which would technically enable the export of tachograph data to other systems and its use for other purposes.

3.2.1.2. LEGAL FRAMEWORK

The legal framework for the Digital Tachograph is Council Regulation 3821/85 of 20 December 1985 on recording equipment in road transport, [35], plus various amendments. The regulation includes detailed functional specifications of the recording equipment and the different types of smart cards for use of and interaction with the device. It also addresses what data are to be logged and under which conditions. It is worth noting that the adoption of the tachograph regulation took place before the data protection directive was adopted. This explains why the regulation is not fully in line with the latter directive.

Currently, a new amendment on the tachograph regulation is foreseen that relates to new technology and new, abovementioned functions of the device.

3.2.1.3. LEGAL BASIS FOR THE PROCESSING

The legal basis for the processing of personal data is of type LB1; a European regulation requires that specific categories of vehicles are equipped with the Tachograph, which locally stores detailed trip data that can be accessed, by drivers, companies, workshops and national enforcement officers with specific authorisation.

3.2.1.4. TERMINOLOGY

The following specific terminology is used in the discussion of this application:

Digitach: digital version of mandatory equipment in trucks and buses for the enforcement of driving hours restrictions.

3.2.1.5. HIGH-LEVEL APPLICATION ARCHITECTURE

The Digital Tachograph is a stand-alone device. It receives information from various sensors in the vehicle. Based on the sensory input, the device determines driving and resting times, which are stored on the head unit's internal memory. Currently, the only interface to extract information from the head unit's memory is through the chipcard slot.

Different chipcards are available; one for each role in the value chain. Depending on the chipcard type, different types of information can be retrieved from the device.

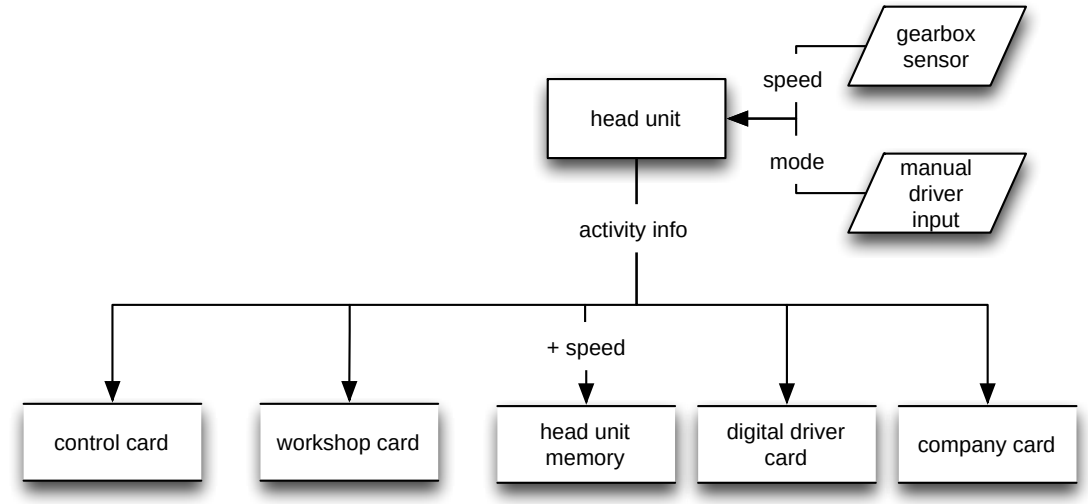


Figure 1 Global technical architecture of the Digital Tachograph

3.2.1.6. CATEGORIES OF PERSONAL DATA INVOLVED

The digital tachograph records a number of features. The most relevant from a personal data protection point of view are:

- Insertions and Withdrawals of Tachograph Cards (this also indicates which driver controlled the vehicle during at what point in time)
- Speed: Details of overspeeding events
- Distances. Odometer readings are stored on a daily basis.
- Time. All log entries are registered with time.
- Drivers' Activities: Recorded in Real Time & Recorded through Manual Entries (Driving, Break/Rest, Available, Work or specific/manually entered)

It is important to note that the existing tachograph does not measure or record positions. The information can therefore be classified as:

- B1: distances travelled are recorded, but not of individual trips. Also periods of driving/rest/co-driving availability are recorded.
- C/C*: other data relating to driving behaviour, in particular speeding information. This may reveal violations of maximum speed and driving hour regulations.

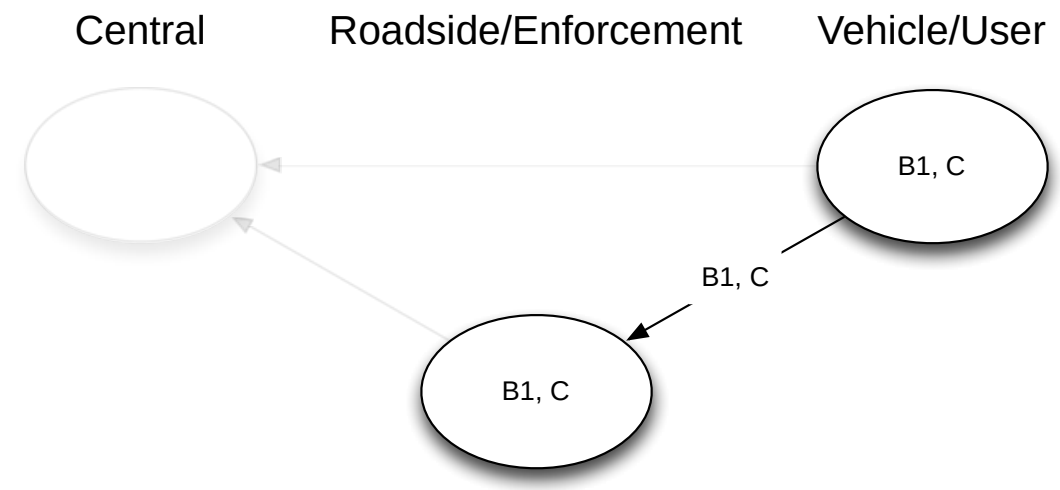


Figure 2 Global representation of storage and exchange of personal data in the different domains of the Digital Tachograph.

The proposed modifications to the Tachograph regulation would lead to inclusion of a GNSS receiver and add position data to be processed. Position data would only be stored for start and end of the daily use of the vehicle. This would add data category A1 to the list above.

3.2.1.7. DISCUSSION

The existing Tachograph regulation and deployment does not seem to have major data protection issues.

The European Data Protection Supervisor (EDPS) raised a number of concerns regarding the proposal for amendment of the regulation, [36]. A generic concern is that the new functionalities introduced are not (yet) covered by detailed specifications in the annexes. This may, according to the EDPS, give way to privacy-unfriendly implementations. The EDPS also observed a lack of precision on security requirements and claimed that a privacy impact assessment should be done before adopting any amendment. Specific concerns are:

- That the GNSS information would be used for permanent localisation (e.g. monitoring of employees by the employer), whereas only a start and end position is required for the legitimate purpose set out by the regulation.
- That the remote compliance checking interface would lead to continuous remote access to the information in the equipment. The proposal includes the following safeguards however: (i) such remote access is restricted only to the competent control authorities; (ii) the scope of the data exchanged with control authorities shall be limited to those strictly necessary for targeted roadside checks; (iii) there is a clearly defined short retention period of two hours of the data gathered during remote checks; (iv) information about the possibility of remote controls shall be

provided to drivers by the owner or holder of the vehicle; and (v) appropriate security measures must be implemented to ensure data integrity and authentication.

- The combination of driver card and electronic driving license may lead to excessive processing of data in processes where only the driving license is to be inspected.
- The ITS-interface implies a risk that the further processing of data recorded or produced by the tachograph for use in other applications would not be incompatible with the original purpose of collection. This must be assessed on a case-by-case basis. The EDPS underlines that amongst all the legal bases available, consent of drivers may be difficult to rely upon, considering the employment context within which the processing operations take place. Drivers might be pressed by their employer to use certain ITS applications for which they would therefore not have given their truly free consent.

As to the last point, one might argue that the assessment of the legal basis for the introduction of fleet monitoring is a separate issue where it seems rather subordinate whether fleet monitoring equipment is connected to the Digitach through the ITS interface or operates autonomously (i.e. uses its own sensors). It does seem relevant that the driver is aware of any systems connected to the Digitach, their purpose and the data exchanged.

3.2.1.8. MAJOR THREATS AND DATA PROTECTION MEASURES

For the Digitach T3 (excessive processing) seems most relevant, although the information that can be produced by the current version is quite limited. T3 is therefore considered to be a medium level, and T1 and T2 low level threat.

T2 (unlawful secondary use) could come into play if the proposal for amendment of the regulation, [36], would be adopted, mainly in relation to the ITS interface.

The following privacy enhancing measures are of specific relevance to the Digitach:

- M3: data minimisation
- M4: domain separation
- M7: distributed processing.

3.2.2. ECALL

3.2.2.1. BRIEF DESCRIPTION

The eCall initiative has been set up with a view to dealing with emergency situations, for which the intervention of emergency services is necessary (e.g. firemen, ambulance, etc). When a vehicle gets involved in a serious crash, the eCall system will trigger a voice call to a so-called Public Safety Answering Point and automatically send basic data on the accident, including vehicle ID and

location of the vehicle. This should lead to a faster and better adapted response of the emergency services. The eCall service is therefore expected to lead to significantly less road casualties.

eCall will be mandatory for new passenger cars and light commercial vehicles as of 2015.

3.2.2.2. LEGAL FRAMEWORK

The data protection directive, [4], applies to the processing of personal data involved in the eCall service. As far as the operations of the mobile communication provider are concerned, the ePrivacy directive applies, [9].

A specific EU regulation on eCall that will also address specific personal data protection aspects is under preparation.

3.2.2.3. LEGAL BASIS FOR THE PROCESSING

It is assumed that the eCall service will become mandatory and therefore have LB1 as a legal basis. Before such legislation enters into force the service will have a voluntary character (LB2).

It is noted that the EU decision for mandatory inclusion of eCall functionality in new vehicles as of 2015 does not imply that the service cannot be switched off. This is still subject to debate, with the above assumption as most probable outcome.

3.2.2.4. TERMINOLOGY

The following specific terms are used in this section:

- PSAP, Public Safety Answering Point: the entity that initially receives the emergency call triggered by the eCall activation.
- MSD, Minimum Set of Data: the data sent to the PSAP in the context of the eCall service, without any additions for value-added services. The MSD contains the time of the incident, the position and driving direction of the vehicle, the identity of the vehicle (Vehicle Identification Number: VIN), some qualification of the severity of the incident, the service provider and optionally the type of fuel. The MSD is defined in EN 15722, [57].

3.2.2.5. HIGH-LEVEL APPLICATION ARCHITECTURE

The eCall initiative has been set up with a view to dealing with emergency situations, for which the intervention of emergency services is necessary (e.g. firemen, ambulance, etc.). For an eCall to take place, it requires the involvement of a number of actors, from the implementation of the eCall platform in the vehicle up to the handling of an actual eCall, namely: (i) vehicle manufacturers who provide the eCall in-vehicle platform, (ii) mobile network operators who ensure the conveyance of data and communications from the in-vehicle platform to the recipient of an eCall, (iii) the Public Safety Answering Point (PSAP) which is the

recipient of the eCall and of the eCall data, and (iv) the emergency services which will be providing the required emergency assistance to individuals in the field, which may not necessarily be the same as the PSAP.

The figure below provides a generic description of the technical architecture of eCall. Based on input from the vehicle's sensors and manual input, the eCall unit decides when to contact a PSAP. The PSAP will receive data describing the vehicles position, status and optionally additional information and/or a voice connection to the vehicle. The PSAP will temporarily store eCall data in its back office system for reference purposes and as input to incident analyses.

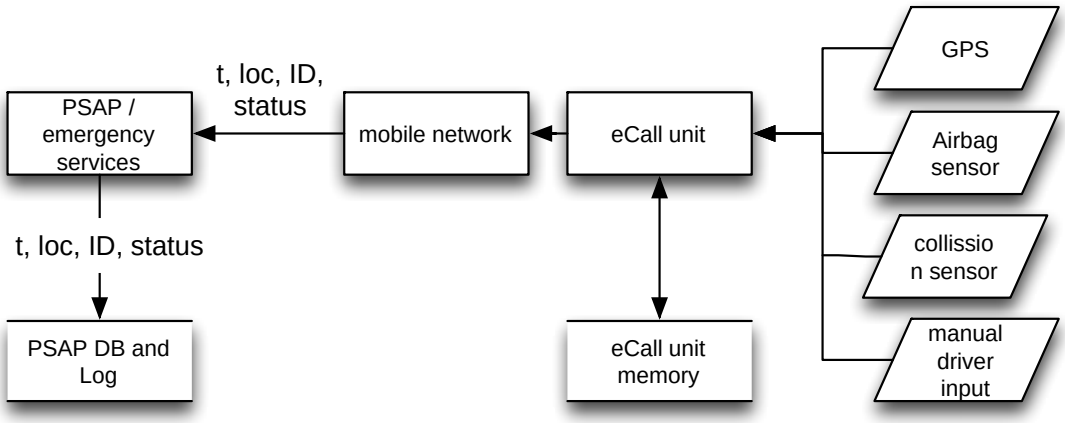


Figure 3 Global technical architecture of eCall. The exact implementation will vary between the MS and providers of the in-vehicle solution. Abbreviations used : t=timestamp, loc=geographic location.

3.2.2.6. CATEGORIES OF PERSONAL DATA INVOLVED

The following data are involved in standard eCall:

- A1: Occasional single samples of position and time
- C*: Details of driving behaviour, at least the fact that an incident has taken place, and some related information. This information is to be regarded as sensitive.

Private eCall or advanced eCall services may process additional data. Such services will also involve additional actors (e.g. vehicle manufacturers, insurance companies etc.).

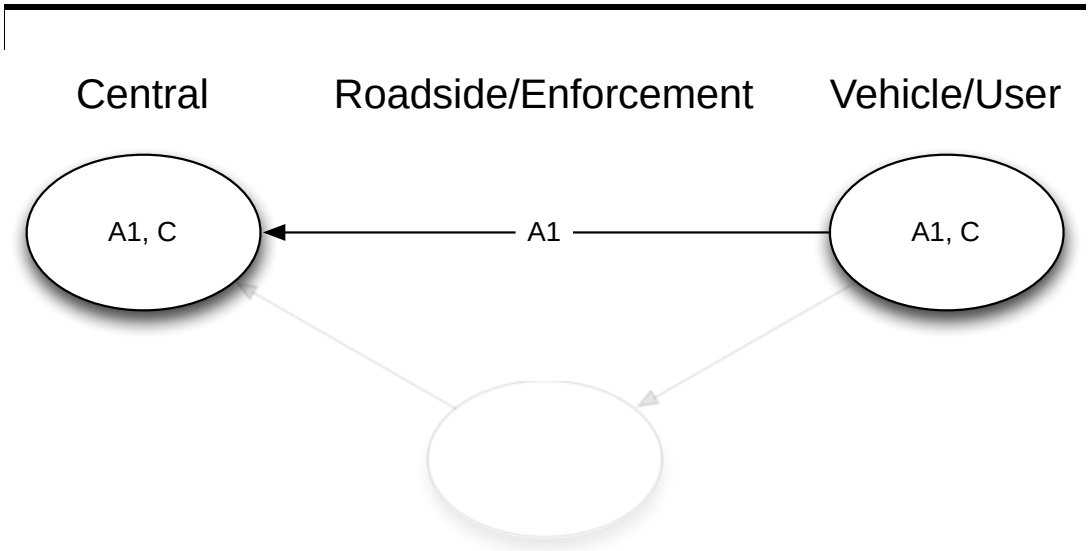


Figure 4 Global representation of the storage and exchange of personal data in the different domains of the eCall value chain

3.2.2.7. DISCUSSION

The eCall initiative has been subject to a specific opinion of the EDPS, see [55]. The EDPS notes that the complex chain of actors (at least vehicle manufacturers, mobile network operators, PSAPs and emergency services) involved does not yet provide clarity on what the respective responsibilities for processing personal data would be. In basic eCall, the Art. 29 WP regards the PSAP as data controller, see [56]. For private forms of eCall, aiming at additional assistance services, the provider of such services would likely to be considered the controller for the processing of the data involved. Specific EDPS recommendations are summarized below.

- Specific modalities, involving one or more actors in the chain, shall be elaborated to ensure that the individual is adequately informed on the processing and the exercise of their rights concerning personal data processing.
- *Permanent tracking of the vehicle is not needed for the purpose and shall be avoided.* The data are only to be exchanged in case of an emergency.
- Only a strict minimum of data shall be processed by the mobile network operator and sent to the PSAP as part of delivering the basic eCall service. This is defined as the Minimum Set of Data
- As to advanced (or extended) eCall services that may also process additional data, this shall be based on a valid legal basis, most probably explicit informed consent of the user. In general the processing for such services shall comply with [4]. This also implies that the data processed shall be minimal with regard to the purpose of each service: an en-bloc

transfer of a full set of data shall be avoided if not needed for the specific service invoked.

- Considering the potential risks to privacy and data protection, the EDPS recommends that the development of advanced eCall applications should be subject to a Privacy Impact Assessment, to be carried out by the data controller/operator of the system.
- Furthermore, the EDPS underlines that appropriate rules on the handling of personal data relating to eCall should be defined not only in respect of mobile network operators but also for all other actors involved. In the context of the regulatory approach of the Commission to eCall, and to ensure consistency and legal certainty across Europe, it would be advisable to have these rules defined at European level.
- The design of the in-vehicle platform should be based on the principle of "privacy by design"; vehicle manufacturers will bear some of the responsibility for the design of the in-vehicle platform, or at least in the choice of specific in-vehicle devices, and they will have to ensure that the device embedded in the vehicle is privacy friendly.
- Furthermore, all the data protection principles should be duly taken into account in developing **detailed rules** on the handling of data in eCall. Particular attention should be given to the following data protection aspects:
  - the categories of personal data processed (MSD or additional data necessary for the provision of additional services)
  - the time limits for the retention of eCall data applicable to the various operators
  - the security measures adopted to protect the confidentiality of the data and to secure the system against unauthorised access and misuse; the feasibility of encrypting eCall data should be explored.

The recommendations, [56], of the Art. 29 WP are in line with, and fully covered by the EDPS opinion.

3.2.2.8. MAJOR THREATS AND DATA PROTECTION MEASURES

The following threat areas are deemed of specific relevance:

- T3: Excessive processing, i.e. processing more personal data than required for the purpose. The risk is classified as medium, as the information is sensitive, but the occasions where information is to be forwarded from the vehicle to the PSAP are rare.

The following measures are of specific relevance to this application:

- M3: data minimisation
- M5: user consent mechanisms

3.2.3. ROAD USER CHARGING

3.2.3.1. BRIEF DESCRIPTION

Collecting fees for the use of the road has been around since Roman times. Traditionally, road tolls were to be paid in cash at a toll booth. A barrier would deny access to the tolled road to people refusing to pay. With the emergence of multi-lane toll highways from the 50's, toll plazas had to be constructed to avoid queues at entries and exits. Self-service payment lanes were introduced on toll plazas from the 60's, featuring coin baskets and later credit card readers. Although the self-service payment lanes helped to reduce costs, it did not solve the problem of congestion at busy toll plazas, requiring many toll booths to take full advantage of the capacity of the tolled road. In the early 80's the first single-lane Electronic Fee Collection systems were introduced. This allowed drivers to pass the toll plaza without stopping, although at reduced speed and an automatically controlled barrier would still manage the access to the toll road.

Developments in the field of radio-frequent identification (RFID) and automatic number plate reading (ANPR) technology enabled the implementation of free-flow Electronic Fee Collection (EFC) systems, also known as ORT (Open Road Tolling). First truly free-flow toll systems were realized in the US, Singapore and Australia. Vehicles could travel across the tolled road network without stopping, provided they are equipped with an electronic tag linking to a valid contract. Roadside systems (located at entries/exists or in the middle of a road segment) read the ID stored in the tag and store this information with location, time and date (and sometimes vehicle classification data) to invoice the user or debit the fee from a prepaid account. In Europe free-flow EFC was introduced in several countries, for Heavy Goods Vehicle charging on the complete main road network. From a data protection point of view, the step from mixed manual-electronic to fully electronic is an important one, as the option of anonymous use of the tolled road is no longer offered in the latter.

In the last decade a new approach has emerged: tolling based on autonomous in-vehicle equipment. In such a concept roadside infrastructure to register tags / observe vehicles is not required, as the OBE itself collects the information needed to calculate the charge. The equipment uses GNSS (generally GPS) to locate itself and cellular communications to sends information on usage of the road infrastructure to the backoffice. Examples of such systems are the LKW-Maut system in Germany and the HGV charging system in Slovakia.

The advantages of free-flow EFC are obvious: no delays for the user to access the infrastructure, no need for spacious toll plazas and usually considerably lower operational costs for the toll operator. There is a drawback as well: EFC without the alternative of cash payment means that data are collected that are usually traceable to an owner or user of the vehicle and that contain information on his

movements (time & location). Depending on the size of the tolled road network and the charging concept mobility patterns – or parts of these - can be derived from such data. Such data are felt to be sensitive by many individuals. It is noted that this perception of sensitivity is not always evident when dealing with professional transport (Heavy Goods Vehicles etc.).

Several countries are – or have been – studying the possibility or even seriously planning Road User Charging (RUC) based on travelled distance for passenger cars on main roads or the complete road network (the Netherlands, Denmark, Belgium, Slovenia, the USA). Distance-based charging on extended road networks is generally seen as a fairer allocation of costs compared to common time-based or fixed charges, and a potentially effective instrument to reduce congestion and reduce the detrimental environmental effects of vehicle use. Realization of such concepts proves to be difficult however, both technically, legally and politically. A consistently major issue is the protection of the privacy of the road users. As long as drivers associate regard EFC as a tool for governments to monitor their private life even more – in extremis enabling governments / operators to follow the car user everywhere he goes – it will be very difficult to get sufficient public support. Convincing measures are needed to take away the fear for 'big brother'.

3.2.3.2. LEGAL FRAMEWORK

No overall specific legal framework. Specific legal arrangements are in place in national or local legislation for individual road user charging schemes.

3.2.3.3. LEGAL BASIS FOR THE PROCESSING

The legal basis for RUC schemes differs per deployment scheme. In some cases, see also 3.2.3.1, electronic payment is offered as an alternative of comfort to manual payment at a tollbooth. This is mostly the case in toll systems that were set up to finance road infrastructure. Many examples are found across Europe, e.g. in Italy, Spain, Portugal and France. The legal basis in this case is LB2: explicit consent of the user.

In other cases there is no alternative to electronic registration (electronic payment and/or ANPR) in case the road infrastructure is used. This is the case the congestion pricing schemes in London and Stockholm and the HGV charging schemes in e.g. Austria, Germany, the Czech Republic, Poland and Slovakia. In these cases the legal basis is of type LB1, i.e. the basis for the processing is provided by dedicated legislation.

3.2.3.4. TERMINOLOGY

The following specific terminology is used:

- Electronic Fee Collection (EFC):

- Toll Charger (TC): entity responsible to charge tolls for the use of a toll domain. The Toll Charger is also responsible for compliance checking and enforcement.
- Toll Service Provider (TSP): entity offering the service of electronic payment to road users. This normally includes the provision of an OBE. An EETS provider is a subtype of a TSP.
- Toll Operator: entity processing toll data in an EFC system, fulfilling the role of TC or acting on behalf of a TC, possibly also fulfilling the role of TSP.
- On Board Equipment (OBE): equipment to be installed in the vehicle which is required for electronic registration by the roadside or for the collection of data to declare tolls electronically.

It is noted that the separation of roles between TSP and TC does not always exist in today's toll schemes: there is often one entity that charges the toll and operates the issuing of OBE, processing of usage data, sending invoices etc.

The European Electronic Toll Service requires that in the future TCs accept certified EETS providers to provide the toll service on his domain (with the exception for local schemes and schemes that use no electronic in-vehicle equipment).

Both TC's and TSP's process personal data.

3.2.3.5. HIGH-LEVEL APPLICATION ARCHITECTURE

The different tolling schemes result in a broad set of possible architectures. In a DSRC based solution, one or more roadside units capture the IDs of passing vehicles, which are relayed to a central system. Based on the roadside data, the central system determines the fee, and takes care of fee collection. It is noted that the depicted architecture assumes that there are no separated roles of TC and TSP. In practice this may or may not be the case.

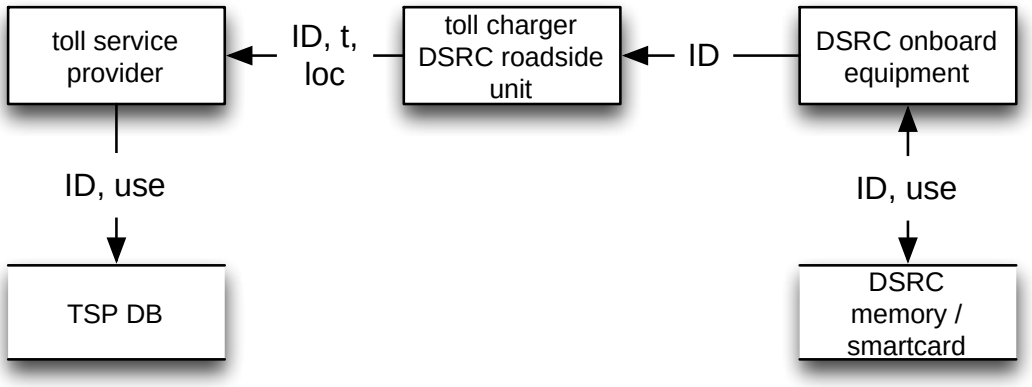


Figure 5 Global technical architecture of DSRC-based road user charging. The exact implementation will vary between tolling schemes. Abbreviations used: t=timestamp, loc=geographic location.

ANPR-based road user charging systems operate in a similar way as DSRC-based systems, except that there is no on-board unit.

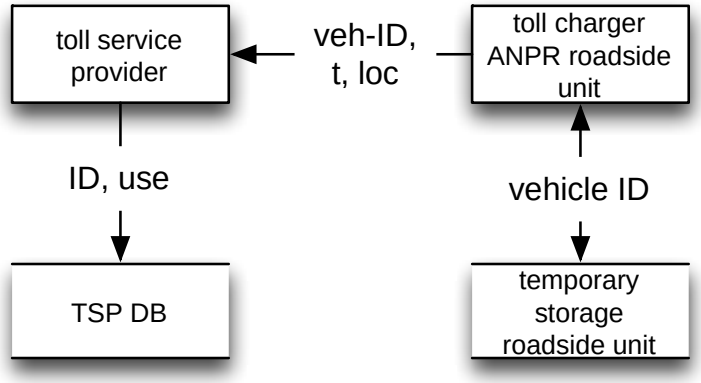


Figure 6 Global technical architecture of ANPR-based road user charging. The exact implementation will vary between tolling schemes. Abbreviations used: veh-ID=vehicle identification, t=timestamp, loc=geographic location.

In GNSS-based road user charging systems, an on-board unit collects sensor data. Different architectures can be designed based on thin, thick and smart client concepts. The architecture described below assumes a thick client, providing only the minimum amount of data to roadside and central systems.

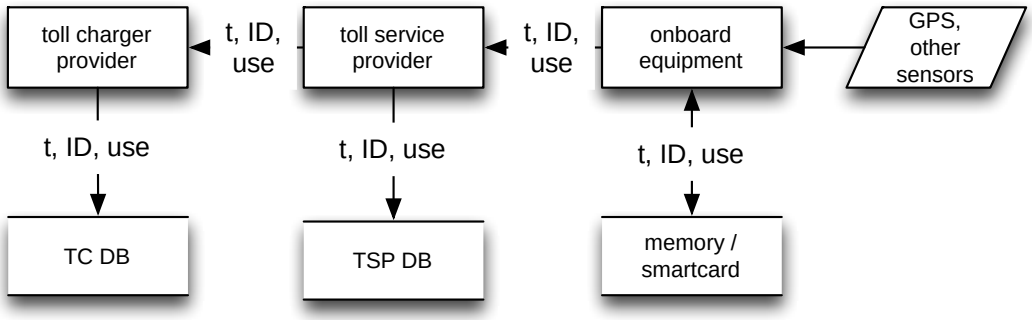


Figure 7 Global technical architecture of GNSS-based thick client road user charging. The exact implementation will vary between tolling schemes. Abbreviations used: ID=vehicle or user identification number, t=timestamp or period.

3.2.3.6. CATEGORIES OF PERSONAL DATA INVOLVED

The category of data processed depends on the extension of the tolled network.

- In the case of a single tolled object, e.g. a bridge or a tunnel, this would classify as category A1: occasional single samples of position and time.
- A road pricing scheme as in Stockholm with multiple registration points would classify as A2: connected samples of position and time, allowing partial reconstruction of routes.

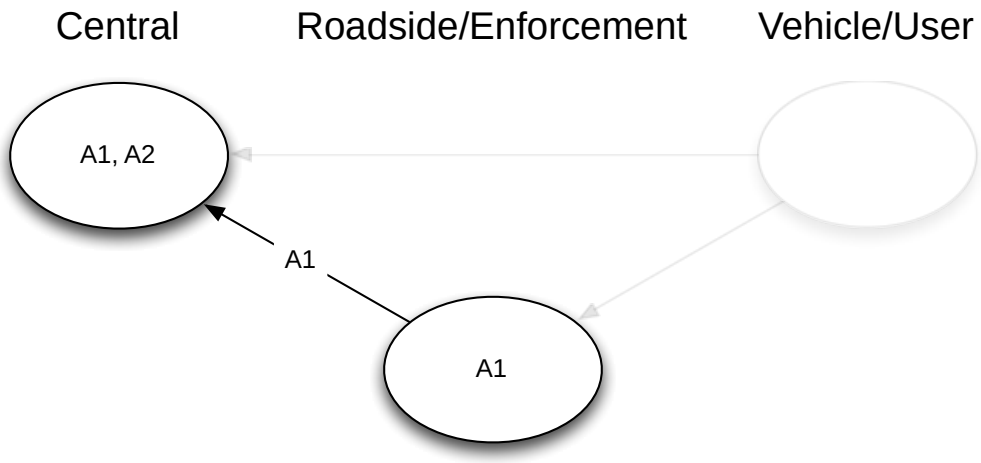


Figure 8 Global representation of the storage and exchange of personal data in the different domains of the value chain of a DSRC- or ANPR-based RUC solution with multiple registration points.

Strictly spoken this also applies to the HGV schemes that charge complete national motorway networks, although it may effectively come close to A3.

- A3 would apply to a charge on all roads, although the information that is processed centrally may be aggregated to category B2 (e.g. only distances reported). There are no operational examples of such a charging scheme. Advanced plans in the Netherlands where abandoned in 2010.

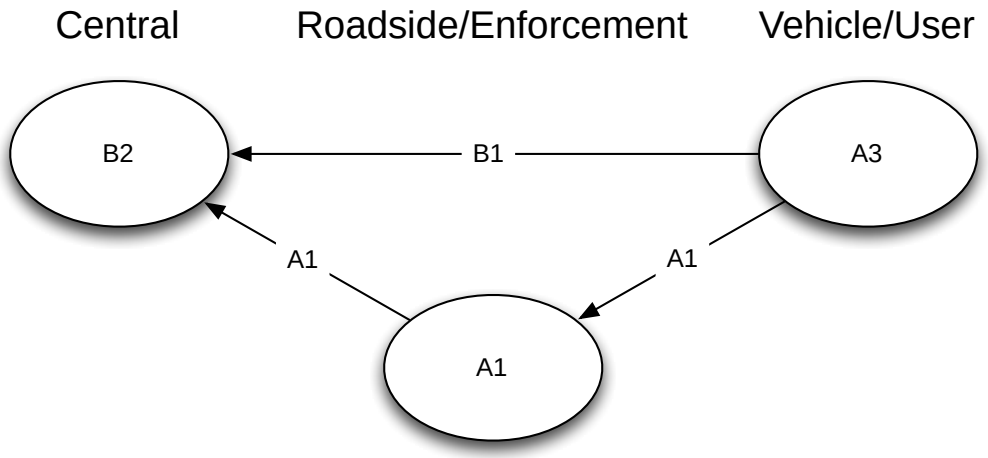


Figure 9 Global representation of the storage and exchange of personal data in the different domains of the value chain of a GNSS-based RUC solution.

Some other personal data are generally processed which do not significantly add to the sensitivity. Such data include the vehicle class or relevant vehicle parameters and an identification of the TSP and information on the correct functioning of equipment and/or recent transactions for compliance checking purposes.

3.2.3.7. DISCUSSION

Road user charging schemes deployed in Europe have a wide variety in terms of objectives, legal basis, characteristics of the toll domain, types of vehicles subject to the charge, number of users, revenues and technology used. It is consequently difficult to define recommendations that would have generic applicability, other than the criteria, conditions and obligations from the data protection directive.

It should be noted that a number of opinions and advices are available that all address an extreme form of road pricing, i.e. distance-based charging for passenger cars on all (major) roads. It is obvious that such scheme would also imply the greatest challenges for user privacy. It should also be noted that no country has yet implemented such a system. The so-called Sofia memorandum of the IWGDPT, [58], contains the following recommendations on 'large scale' road pricing:

1. The anonymity of the driver can and should be preserved by using the so-called smart client or anonymous proxy approaches that keep personal data of the drivers under their sole control and do not require off-board location record-keeping.
2. Road pricing systems can and should be designed so that the detailed trip data are fully and permanently deleted from the system after the charges have been settled in order to prevent the creation of movement profiles or the potential for function-creep.
3. Processing of personal data for other purposes (e.g. pay-as you drive insurance or fleet monitoring), should only be possible with clear and unambiguous consent from the individual.
4. In terms of enforcement, the system should not ascertain the identity of the driver or owner of a vehicle unless there is evidence that the driver has committed something which is defined as a violation of the road pricing system.

These recommendations would have a large impact and need to be further discussed:

As to points 1 and 2: It is noted that the phrasing 'preserving the anonymity of the driver' seems a bit misleading. A smart client approach avoids central processing

of detailed location and trip information which would be a strong advantage from a personal data protection point of view. This view is completely in line with earlier opinions of the Slovenian and Dutch data protection supervisors, see [59] and [60]. However, at least aggregated information required for billing is still to be uploaded to the TSPs backoffice. Such information is by definition linked to a contract holder and cannot be regarded as anonymous. It should further be noted that the fact that detailed information is processed in the OBE and not uploaded to the backoffice does not mean that these data are not processed under the responsibility of the controller. In other words, it does not imply data minimisation, it is a measure of distributed processing. When applying a smart client concept, the question gets relevant who actually controls the OBE. In the political debate around the Kilometre Price in the Netherlands in 2009/2010, the proposed smart client concept was still vulnerable on the aspect of privacy, although it was in line with the advice of the data protection supervisor. A major concern was that as long as the device is remotely ('over the air') controlled by an entity that cannot be trusted to always give privacy a higher priority than other business interests (e.g. reducing fraud), there is no guarantee that settings or software will not be changed at some point to upload locations / movement details after all. In theory this can be solved by an OBE which is not part of the controller domain but owned and fully managed by the user, reporting to a backoffice strictly the information the user consented to. The (software) management, customer service, compliance and security issues involved seem too great an obstacle at the current state-of-the-art however.

Another factor that adds to the complexity of the issue is that reporting of aggregated amounts or distances only may serve the primary process and the 'happy flow', i.e. the flow of actions and data when everything works as expected. For considerable numbers of users, an itemised invoice would be an absolute requirement for accounting or reimbursement purposes. Furthermore, the correct measurements of the OBE (or its inputs, in particular GNSS receiver data) or the billing process of the TSP cannot be guaranteed in absolute terms. In order to protect the user against erroneous bills, he should have some additional information at his disposal. Furthermore this information is to be provided with proofs of integrity and authenticity in order to be of use to substantiate a complaint or appeal. This can be accomplished with a 'user log' with digitally signed entries at the disposal of the user, as was proposed in the Dutch Kilometre Price Act, see [60] and [61]. To strengthen the concept and perception of user control, these data should never be available to the processor unless presented – requiring explicit action – by the user. The OBE holder would also have the possibility to delete (part of) the data in the user log.

As to point 4. This recommendation addresses the actual identification of the person driving or owning vehicle, it does not mean that no personal data are processed in the process of compliance checking. It is noted that compliance checking communication using DSRC for autonomous OBE based charging

systems, as standardised by [62], cannot be regarded an anonymous process as the information will include an identification of a service provider and contract ID.

The large-scale and innovative forms of road pricing the quoted opinions/advices relate to, have not yet been realised in practice. Meanwhile numerous implementations of tag-and-beacon based road pricing schemes have been realised. In such schemes, no option for a 'smart client' solution exists (as the concept is based on identification by the roadside equipment) and it seems a 'fait accompli' that complete logs of passages are processed by the respective operators. It is noted that the privacy issues can often be regarded of a smaller order of magnitude as the schemes for passenger cars are often small-scale or offer electronic payment just as an option of convenience, and the privacy of the users in the schemes exclusive for HGV is in practice much less a concern. Still there seems to be room for data protection supervisors to provide more clarity and guidance as to personal data protection in the area of road pricing.

3.2.3.8. MAJOR THREATS AND DATA PROTECTION MEASURES

All identified threat areas are of specific relevance to road user charging:

- T1: Unauthorised access to personal data, by eavesdropping, unauthorised actions of staff, hacking etc. This is classified as a medium risk as some usage information has to be kept centrally for billing purposes. This information does not have to be very detailed.
- T2: Re-use of personal data beyond the legally defined purpose or beyond the scope of the consent of the data subject. This holds in particular for GNSS based solutions which can produce commercially interesting by-products such as traffic speeds and travel times for large areas.
- T3: Excessive processing, i.e. processing more personal data than required for the purpose. This applies in particular for GNSS based solutions as at least initially, very detailed geolocation data are available. The risk is deemed lower for ANPR and DSRC based solutions in which by definition only data are available from observation/communication points.

The following measures are of specific relevance to road user charging:

- M3: data minimisation (all types)
- M4: domain separation (all types)
- M7: distributed processing (if GNSS-based)
- M8: data subject control (if GNSS-based)

3.2.4. ETICKETING IN PUBLIC TRANSPORT

3.2.4.1. BRIEF DESCRIPTION

In the past decades electronic fare collection has been introduced on a large scale in public transport systems across Europe. Schemes have been introduced in major cities such as London, Paris and Berlin but also in medium-sized cities and regions. The Netherlands have introduced a nation-wide scheme that includes all modalities and public transport companies. Denmark is also planning a nation-wide scheme.

The (assumed) benefits of electronic fare collection are the following:

- Improved resource management as complete and detailed vehicle occupation and source-destination information becomes available
- Better information for strategic public transport planning
- Possibility of accurate apportionment of revenues between operators that have shared fare products
- Reduction of fare evasion, higher compliance rates with less enforcement effort
- Cheaper processes to issue tickets
- More flexibility in tariff settings
- More options for profiling and marketing
- Ease of use for the customer
- All adding to a better service offering, better image of public transport, possibly resulting in attraction of new customer groups.

It is noted that it does not prove easy to realise all these benefits in practice.

There are large differences between schemes. A common characteristic is that a so-called Customer Medium (often a chipcard) is used to carry transport credits and/or travel rights in electronic form. An important characteristic is the boarding regime, which is either Check-In-Check-Out (Customer Medium to be presented to a validator at entry and exit) or Check-In-Only. A comprehensive overview of e-ticketing in public transport can be found in [51].

[50] summarizes the challenge of personal data protection in e-ticketing systems as follows:

“The online purchasing of tickets in the transportation sector poses challenges in the way how (and whether) the principle of minimal disclosure is respected in this field. [...] Users tend to reveal a large number of personal information and leave traces of their location at various time points for the sake of “convenience”. [...] The unique number that is stored on the card allows for the tracking of the location of the user and, when combined with the identification data of the user that may be revealed when the electronic ticket card has been purchased via a credit or debit card, it offers a rich amount of personal information that can be used for user tracking and user profiling”.

3.2.4.2. LEGAL FRAMEWORK

No specific legal framework.

3.2.4.3. LEGAL BASIS FOR THE PROCESSING

The legal basis for e-ticketing, when offered as an optional service, is classified as LB2. This is often the case in schemes that are in a process of transition from paper-based to electronic ticketing. The user has the choice to use a paper or an electronic ticket.

The end goal is in most cases however a complete conversion to e-ticketing, as a hybrid system is more complex and costly to operate. In this case the legal ground is to be classified as LB3.

3.2.4.4. TERMINOLOGY

The following specific terminology is used:

- Fare Product: right to travel, or right to reduced tariff which is stored on a Customer Medium
- Customer Medium: device required to use the e-ticketing system, on which Fare Products and travel credits are stored. This is often a chipcard, but since a few years also smartphones may serve as CM in some schemes.

3.2.4.5. HIGH-LEVEL APPLICATION ARCHITECTURE

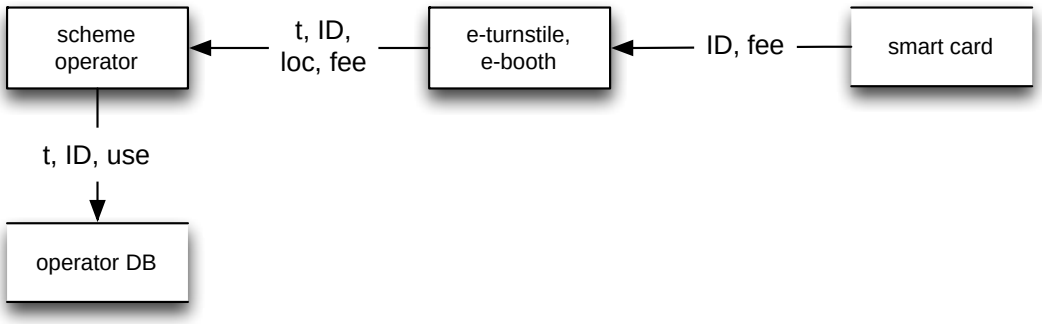


Figure 10 Global technical architecture of e-Ticketing schemes. The exact implementation will vary between the MS and providers of the solution. Abbreviations used: t=timestamp or period, ID=user identification number, loc=geographic location.

eTicketing schemes rely on smart cards carried by the end-users. Service usage is determined by detection of passages of turnstiles or user registration at booths. Transactions and credits can be stored on the smartcard alone, but many schemes collect and store usage data from turnstiles and booth in a central system to monitor usage and detect fraud.

3.2.4.6. CATEGORIES OF PERSONAL DATA INVOLVED

- The personal data involved in e-ticketing are generally of type A2 (connected samples of position and time, allowing reconstruction of trips/routes). Depending on the scale of the e-ticketing the data may be of type A3: complete traces of a natural person. Often, a number of recent transactions is also kept on the Customer Medium. This qualifies as category A2: the information might reveal recent trips in detail, but the history would be limited.

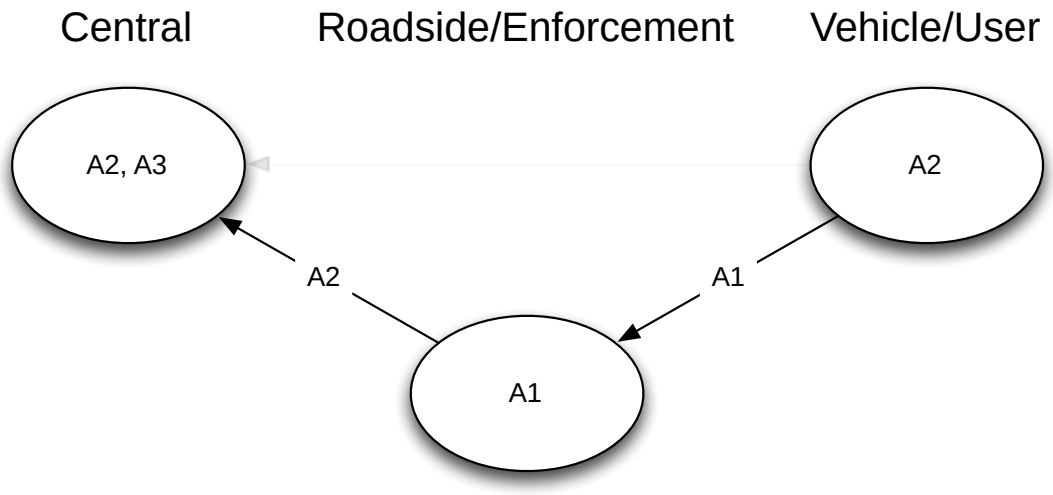


Figure 11 Global representation of the storage and exchange of personal data in the different domains of the e-ticketing value chain.

Some additional information may be linked to the cardholder: reduction rights related to age or social status, specific fare products acquired.

3.2.4.7. DISCUSSION

An important element of the privacy discussions around e-ticketing is always the option to travel anonymously. It seems straightforward that the data protection directive requires that anonymous (no submission of holder details required) Customer Media shall always be offered as an option to the traveller. This is also recommended in the IWGDPT working paper on e-ticketing, see [49]. It might seem that offering a fair alternative that allows travelling anonymously eliminates all privacy concerns. However, there are some important limitations:

- Many public transport operators offer personalised Fare Products, i.e. not valid for any person presenting the CM, but only to a single registered person. This typically applies to expensive fare products that entitle to travel without limitation on a certain network, section or for all services of one or more operators. In order to check that the conditions for use are complied to, these products require a personalised Customer Medium: it should have an ID that is linked to personal identification data

stored on the CM or printed on the outside (optionally including a pass photo). As a consequence, the alternative of an anonymous CM cannot be considered as an equivalent to the personalised CM as certain fare options are not available.

- Similar to Floating Car Data, see 3.2.9.1, it should be noted that even if the card ID cannot be directly be related to a natural person, it is often possible to determine the identity (or a few possible identities) by analysing travel patterns, and possibly a comparison with other databases. Although it will generally require quite an effort to identify the cardholder, the data have to be regarded as personal data. The situation would considerably improve if the service user would be able to change his CM very frequently. The price of the medium is however a major obstacle for such a practice.

It is concluded that the availability of an anonymous CM is recommendable, but does not provide for fully anonymous use of the service.

The CNIL provided a set of guidelines for e-ticketing providers in France, which was updated most recently in 2011, ref. [52]. The availability of an anonymous CM is also included. Further recommendations are summarized below. It is noted that some recommendations are discarded which are regarded to be specific for the given context in France.

1. The cardholder/service user should be adequately informed on e.g. the purposes of the processing, the identity of the controller, the data categories processed, other parties with access to personal data, the right to use an anonymous ticket, and how the rights to inspect data, have errors corrected and have old data erased can be exercised.
2. Anonymous tickets/CM should be available at the same rates and under the same conditions as personalised tickets. (It is noted that this is no issue for the declarative pass available – Navigo découverte – in France).
3. For a personalised CM, the cardholder should have the right to refuse that his picture is stored in digital form.
4. Specific information is to be provided to customers in relation to overdue payment management and blacklisting.
5. 4 legitimate purposes of processing under the authorisation provided: management of transport tickets and payments, fraud & security management, statistical analysis of the use of the public transport services and quality assessment and monitoring of the system. It is noted that profiling for marketing purposes is not included.
6. All personal details that may be processed are specified. Other personal details should not be processed.

7. Data processing shall be anonymised, except when a need exists in the area of investigation or mitigation of fraud.
8. Limitative categories of personnel that would have access to travel and personal data are specified.
9. Public transport companies can only collect the date, the time of use and data which are necessary to calculate the price of the ticket. Data revealing the place where the ticket has been validated (the station of validation) should not be processed as it is not necessary for the calculation of the price.
10. In the case where e-ticket/CM would also be used for services other than the public transport service, the modalities of use must ensure a strict separation between public service transport and any other services. This separation shall guarantee that the service provider will not be able to affect the functioning of other services and it must be possible to inactivate access to all or specific additional services on one's CM.
11. All data can be stored for the full duration of the contractual relationship and, upon the end of it, for two years for commercial and statistical purposes. However data revealing information about the movements of the users shall be anonymised as mentioned in recommendation 12.
12. Validation data that reveal information about the movements of the users cannot be stored, unless in anonymised form. The anonymisation can take place either by completely removing the card number or the joint date, time and place of the journey, or by applying a cryptographic algorithm that does not allow derivation of the card number. Non-anonymised data can be kept for a maximum of 48 hours, for the purpose of fraud investigation and mitigation.
13. Public transport companies shall take all necessary measures in order to preserve data security and confidentiality in order notably to avoid that data are distorted, damaged, or communicated to unauthorized persons. Specific security mechanisms to be implemented are specified.

Some remarks as to the wider applicability of these recommendations have to be made:

- Concerning point 2: as discussed above, this seems to exclude the possibility of fare products that only entitle a single person to specific travel rights.
- Concerning point 5: public transport operators often wish to apply profiling also for direct marketing purposes. This seems acceptable with explicit informed consent of the user. In the case of the Dutch OV-

Chipkaart this triggered a dispute whether an opt-in by default could be regarded as explicit consent.

- Concerning point 12: in an electronic ticketing system, many customers will still have a need to present specified declarations of travel to e.g. an employer or tax authorities. Such information may also be required for purposes of reclaim, in case a check-out was omitted or terminal equipment was out of order. In theory, such information could be available through a log on the CM itself, which could be accessed through a card reader connected to a PC. It is doubtful whether such an approach would be cost-efficient in operation. We note that e.g. in the Dutch national e-ticketing scheme ('OV-Chipkaart') users have access to a central log which provides full details of purchase and travel.

The International Working Group for Data Protection in Telecommunications issued a working paper on e-ticketing with principles to be respected [49]. The recommendations do not conflict with the CNIL guidelines but have a more generic nature. In summary:

1. Privacy-By-Design practices should be adopted in the design of e-ticketing systems and services: e.g. systems shall be designed by prioritizing the use of anonymous data.
2. Anonymity: the Public Transport Authority or transport companies shall provide alternative ways for users to travel anonymously and without undue obstacles.
3. Privacy policy and transparency: users shall be informed on the processing of personal data in a clear and unambiguous manner.
4. Storage period: information shall be stored for the shortest possible period (and erased automatically thereafter), this should be no longer than a few days.
5. Security: an audit system shall be included to prohibit the misuse of information and transport companies shall ensure that the privacy of registered users is guaranteed when making their databases accessible to partners or even their own employees.
6. Marketing: the consent of the user for the use of personal data for marketing purposes shall be distinct from the acceptance of the general contractual obligations.
7. Code of conduct: adoption of code of conducts by the industry shall be encouraged.
8. System Design: central storage shall be reserved for aggregate data and/or anonymous transactions and the cardholder shall be able to control information concerning his use of the card.

The EU FP7 IFM (Interoperable Fare Management) project also specifically addressed privacy issues in e-ticketing, see [83]. This reference lists best practices

concerning personal data protection on a number of aspects. The most important recommendations are summarized below:

1. Transaction data and personal data shall be linked only if this is necessary. Journey data shall be stored separately from other personal data in both an organisational and a technical sense. This is an example of domain separation, see 3.2.4.8.
2. Public transport companies shall enable passengers to view their transaction data and/or journey data via the internet. This is an elaboration of IWGDPT recommendation 3 above.
3. If journey data need to be processed for the purposes of providing a service other than fulfilling the agreement, explicit consent of the cardholder will be asked. This relates to IWGDPT recommendation 6 above (but covers other purposes as well).
4. There shall be a free decision for passengers between anonymous travel and 'special performances' that require personal data. This seems in line with IWGDPT recommendation 2. It is recognised that for some fare products personal data are required, but personal entitlements should not be stored electronically for further processing (in addition to a customer profile on the Customer Medium, and related checks by inspection staff).
5. Specific measures to protect against unauthorised disclosure and modification of data are recommended. This includes access control mechanisms for user access to payment/journey data via vending machines, internet etc.
6. It is noted that the IFM value chain may have a complex mix of responsibilities with multiple processors. The entity defining the purposes and the one defining the means do not always coincide. An overarching role of “privacy manager” is therefore suggested in an interoperable fare domain. The privacy manager can receive a delegation of responsibility for common privacy concerns such as the relations with common suppliers, common sub-contractors or loading agents. He will be in charge to represent the stakeholders of his IFM when discussing privacy issues with another IFM in setting an agreement for interoperability.
7. As to the use of journey data for personalised marketing and promotion purposes, the paper recognises that this development is in the customers' and public interest and should not be blocked by personal data protection restrictions. However, only derived journey data should be used (not indicating details of trips, times and dates etc.). In addition, passengers should always have an opt-out for this type of processing. This seems a weakened elaboration of IWGDPT recommendation 6. It is noted that in some cases data protection authorities indeed ruled that processing of personal data

for marketing purposes should be based on 'opt-in' i.e. explicit consent.

8. Transaction and Journey Data should not be stored longer than needed for contractual and/or legal obligations. Passengers may view their data for a maximum period of 18 months after the travel/transaction took place. This is an elaboration of IWGDPT recommendation 4.
9. The passenger shall be enabled to inspect what personal data are stored by the public transport company. He shall be entitled to request to improve, add, remove or protect data that are factually incorrect, incomplete or irrelevant. The public transport company shall respond to such requests, after proper verification and checking the authenticity of the request. This is an elaboration of IWGDPT recommendation 8.

It is noted that smart mobile devices with NFC (Near-Field Communication) capability will increasingly be used as Customer Media for e-ticketing – this is already deployed in China and India. Whereas a number of data protection issues and solutions would be similar to e-ticketing with a 'single-purpose' medium such as a smart card, additional challenges are introduced by the fact that a personal handheld device will store personal data for many purposes and applications and each will have different mechanisms and measures to share and protect data. Adequate data management and security seems a challenge in such an environment, see also [81].

3.2.4.8. MAJOR THREATS AND DATA PROTECTION MEASURES

All identified threat areas are of specific importance to e-ticketing:

- T1: Unauthorised access to personal data, by eavesdropping, unauthorised actions of staff, hacking etc.
- T2: Re-use of personal data beyond the legally defined purpose or beyond the scope of the consent of the data subject. This risk is ranked high, as the data have great marketing potential.
- T3: Excessive processing, i.e. processing more personal data than required for the purpose. This risk is classified ‘high’, for the same reason as T2.

The following measures are of specific importance to e-ticketing:

- M1: anonymisation
- M4: domain separation
- M5: user consent mechanisms.

3.2.5. PARKING PAYMENT SERVICES

3.2.5.1. BRIEF DESCRIPTION

The advancements in ICT have also reached the area of paid on-street parking. In traditional solutions, parking ticket vending machines (TVM's) provide paper tickets on payment of the amount due for a specified period of parking. The ticket is to be placed on the dashboard, visibly from outside. Enforcement is based on manual visual inspection by parking enforcement staff.

In the past decades, municipalities and parking equipment vendors have been looking for solutions that reduce cash in the machines, reduce fraud, increase efficiency and effectiveness of enforcement and payment collection and may increase the comfort of the car user.

Two innovations are of specific interest to this study:

- *Type 1*: a service to which the motorist has to subscribe and which allows post-payment of the parking fee, based on the actual duration of parking. To activate the service, the user calls the service provider, provides the parking area ID (displayed on signs), his own subscriber ID and PIN. The activation process is generally also available through SMS or a dedicated app. The parking service provider informs the authority that operates or enforces the on-street parking facility that the fee will be paid for the corresponding parking event (VRN, time, area). On-street enforcement officers will have access to this information using their PDA with wireless capability.
- *Type 2*: this innovation applies to all users of the on-street parking facilities. The TVM does not only require a specification of the duration of parking, but also the VRM to be specified. This allows more efficient enforcement as the officer only has to key in the VRM of the parked vehicle on his PDA to check compliance.

3.2.5.2. LEGAL FRAMEWORK

No specific legal framework.

3.2.5.3. LEGAL BASIS FOR THE PROCESSING

Type 1: the legal basis is of type LB2; the user subscribes freely to the service as an alternative to the common payment method.

Type 2: the legal basis should be of type LB3, the legitimate interest of the controller, which exists of an increase in the efficiency/effectiveness of parking regulation enforcement.

3.2.5.4. TERMINOLOGY

Parking event data: stored data relating to the parking of a vehicle, i.e. time and date, VRM and/or subscriber ID, optionally end time.

3.2.5.5. HIGH-LEVEL APPLICATION ARCHITECTURE

The different types of parking payment schemes result in different system architectures. In online parking payment systems, the user provides a vehicle ID and location to the central system of the parking service provider. The parking service provider will store the data for, at least, the duration of the parking period.

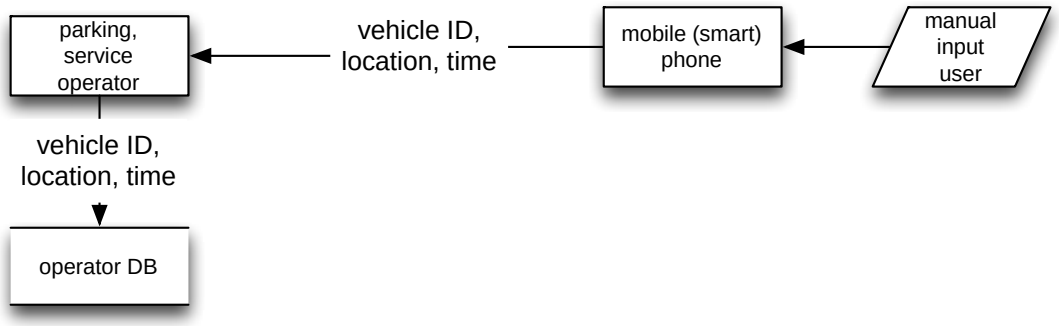


Figure 12 Global technical architecture of online parking payment systems. The exact implementation will vary between providers of the solution.

Parking services that rely on ticket vending machines use a similar architecture, except that a vending machine replaces the user's device as input terminal.

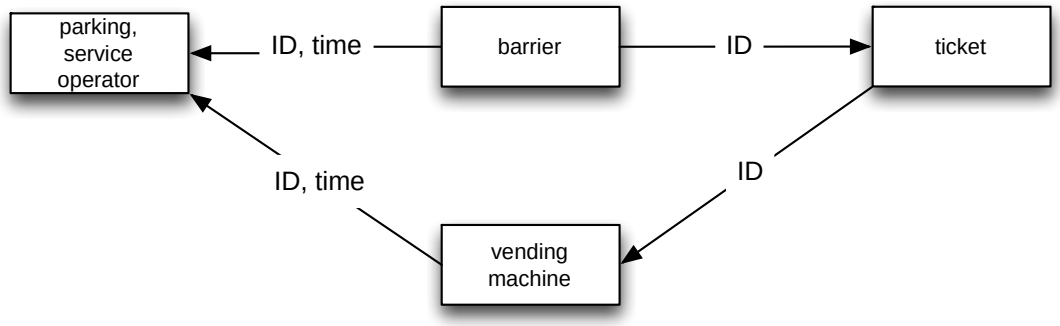


Figure 13 Global technical architecture of parking payment systems based on ticket vending machines. The exact implementation will vary between providers of the solution. Abbreviation used: ID=vehicle identification number.

3.2.5.6. CATEGORIES OF PERSONAL DATA INVOLVED

The categories of personal data processed are of type A1, occasional samples of location and time. Depending on the architecture, the storage locations and interfaces differ between online parking payment, and ticket vending machine based parking payment systems.

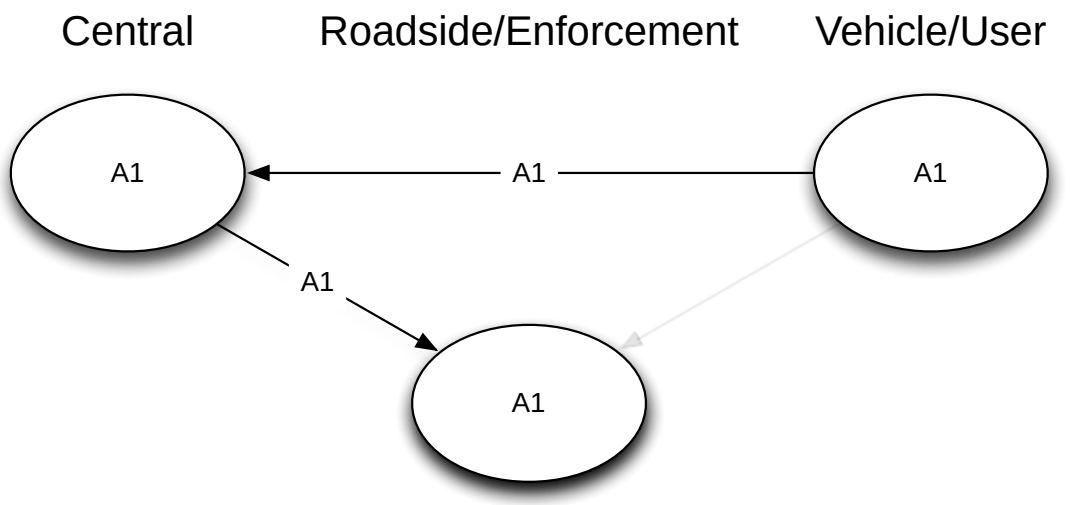


Figure 14 Global representation of the storage and exchange of personal data in the different domains of an online parking payment system. The exact implementation will vary between different parking payment schemes.

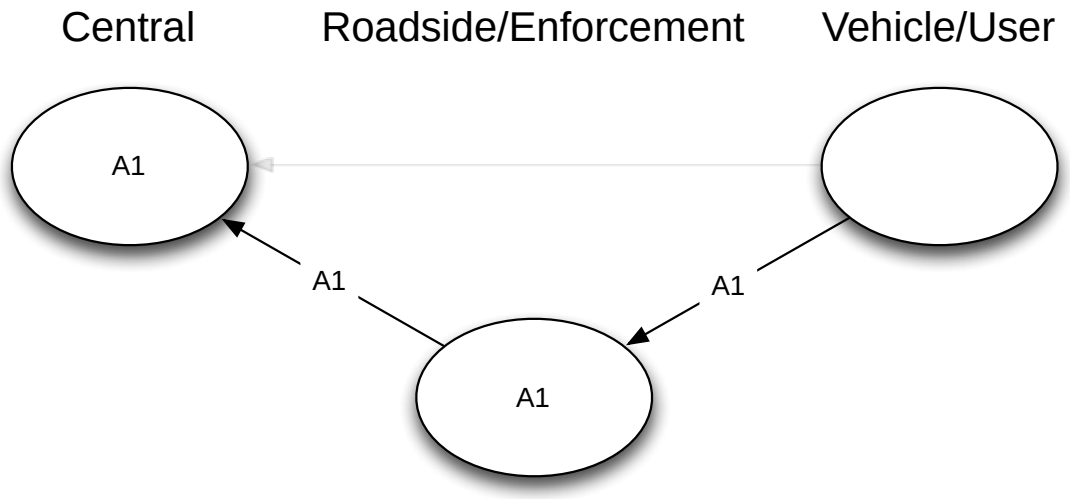


Figure 15 Global representation of the storage and exchange of personal data in the different domains of a parking payment system based on ticket vending machines. The exact implementation will vary between different parking payment schemes.

3.2.5.7. DISCUSSION

Type 1

This parking payment service is completely voluntary. It is required that the subscriber is fully informed on the personal data that are processed to operate the service and that his agreement can be regarded as explicit informed consent.

Other straightforward requirements to the processing are:

- The parking event data are stored no longer than needed for billing and payment (including a period for appeal)
- The parking event data are not used for other purposes (unless explicitly agreed by the user)
- The parking event data are only shared with the parking authority or enforcement operator
- The stored parking event data are adequately protected.

Type 2

The first question is whether the interest of more efficient parking fee collection shall prevail over the privacy infringement caused by a systematic processing of parking events of individual vehicles. No case law was found that addresses this issue for this specific application.

Assuming that this question is answered positively, the following requirements to the processing would apply:

- The parking event data are stored no longer than needed for billing and payment (including a period for appeal)
- The parking event data are not used for other purposes, unless in a fully anonymised form. It is noted that these parking event data are of interest to urban planning and mobility policy. Such purposes do not require the use of personal (identifiable) parking event data.
- The stored parking event data are adequately protected.

3.2.5.8. MAJOR THREATS AND DATA PROTECTION MEASURES

The following types of threats are of specific relevance to this application:

- T2: Re-use of personal data beyond the legally defined purpose or beyond the scope of the consent of the data subject.

The following measures are of specific relevance:

- M4: domain separation
- M6: deletion immediately after initial processing

3.2.6. PAY AS YOU DRIVE INSURANCE

3.2.6.1. BRIEF DESCRIPTION

Pay-As-You-Drive car insurance schemes have as a main characteristic that the insurance premium is based on the driving behaviour of the policy holder. Generally, PAYD ties the level of insurance premium to the risk level associated with driving behaviour of the policy holder. For example, increased mileage and speeding are associated with increased crash risks, and thus can be used to determine the level of the insurance premium. This system of variable premiums poses an alternative to today's common schemes with fixed insurance premiums that are exclusively based on proxies for risk such as age and gender. In addition

to increasing actuarial accuracy PAYD might lead to a change in the driving behaviour of policy holders which is likely to have a positive effect on traffic safety. An overview of PAYD objectives and effects can be found in [44].

PAYD can be classified in terms of the type of data that are used to calculate the premium and the method to measure such data. For the scope of this study, only the more advanced concepts using a 'blackbox' with GNSS and wireless communication capability are discussed. The set of parameters used for PAYD will differ between deployments. Most common as a parameter is the mileage. Other relevant parameters can be the areas where km's are driven, the road type, season, day of the week, time slot and length of the trip. Finally, also details of driving behaviour can be taken into account, e.g. rate of acceleration/deceleration, speed, seatbelt use, duration of driving between periods of rest. It is noted that some of these parameters require dedicated additional sensors in the blackbox or connections to other sensors in the vehicle.

3.2.6.2. LEGAL FRAMEWORK

No specific legal framework.

3.2.6.3. LEGAL BASIS FOR THE PROCESSING

The legal basis for the processing is in the current situation is LB2: explicit consent of the user. PAYD is still to be considered as the exception to conventional car insurance. The vehicle keeper accepts the PAYD regime without any obligation. It is likely that his choice will be influenced if the resulting premium is clearly lower compared to the flat rate.

It is noted that when premiums for conventional insurance would be significantly higher than for PAYD, the concept of free consent would be challenged. [46] also points at this issue.

3.2.6.4. TERMINOLOGY

No specific terminology.

3.2.6.5. HIGH-LEVEL APPLICATION ARCHITECTURE

PAYD requires an in-vehicle device to capture the driving behaviour based on input from various sensors and data on regulations. Privacy-friendly PAYD schemes will only communicate parameters describing driving behaviour, e.g. aggregated for specific time periods and not related to the driving location.

The insurance company, or PAYD service provider acting on behalf of it, will store the data to build the policy holder's track record, which in turn will determine policy conditions.

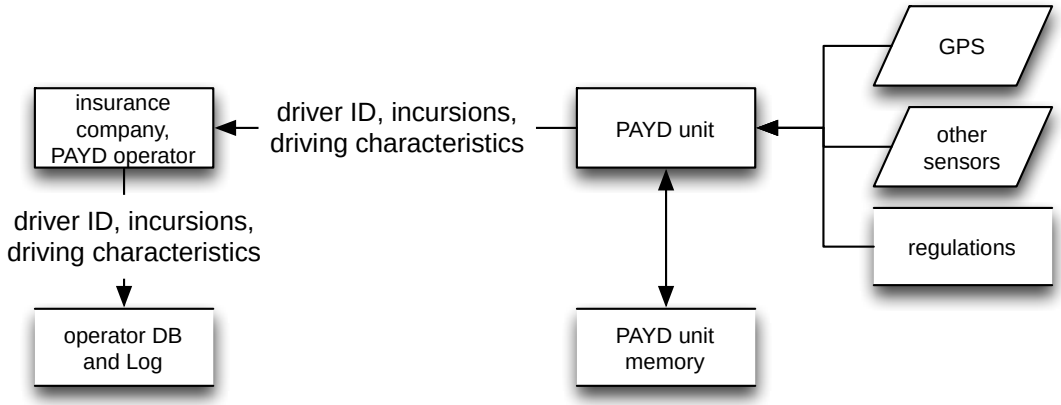


Figure 16 Global technical architecture of PAYD. The exact implementation will vary between providers. Abbreviations used: Driver ID=user identification number.

3.2.6.6. CATEGORIES OF PERSONAL DATA INVOLVED

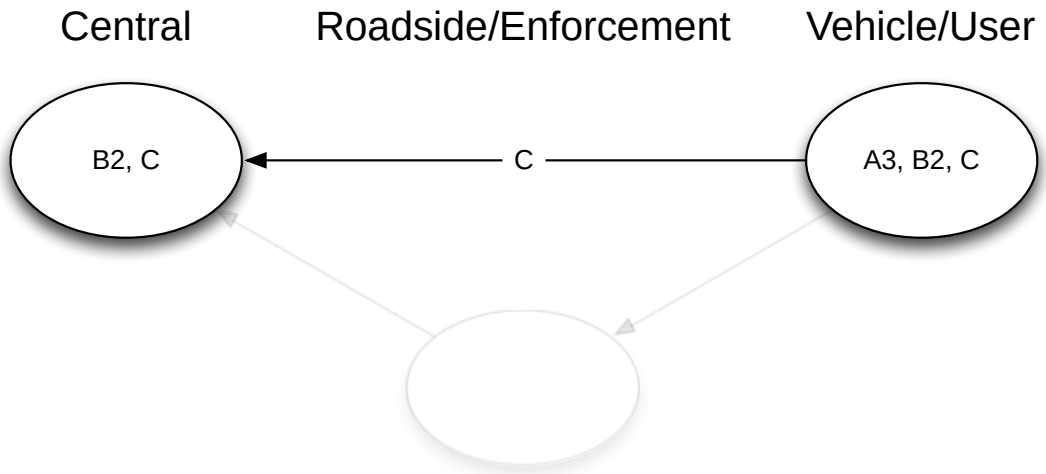


Figure 17 Possible global representation of the storage and exchange of personal data in the different domains of a PAYD scheme.

The categories of personal data processed in a PAYD scheme depend on the parameters that are used. In general the following categories apply:

- A3: Complete location traces of a vehicle, including time and precise location trough GNSS need to be stored at least temporarily on the in-vehicle unit. (Simpler schemes may only register distances travelled, category B2).
- C/C*: Details of driving behaviour (speed, acceleration, brake power applied, seat belt use) are directly measured or derived from A3 and transmitted to the insurance company (or an intermediate). The information may also indicate events of excessive speeding (which is classified as sensitive data C*). It is assumed that such information is not

reported to the central system, or only in an aggregated form (i.e. not reporting specific violations).

3.2.6.7. DISCUSSION

The first aspect to consider is whether the personal data processed through PAYD, and collected by a blackbox, are needed to achieve the purpose of the service. For some parameters the relation with crash risk is evident, for other parameters a correlation is expected but there is insufficient research data to substantiate this. As to the effectiveness influencing driver behaviour in a positive way through possible premium reduction, more research is needed before conclusions can be drawn, see also [44].

One of the early plans for PAYD came from MAAF Assurances S.A. and consisted of new insurance policy for young drivers, who would agree not to drive during the weekend at night or longer than two hours as well as not to exceed the speed limit. To check compliance with the policy the insurance company would collect data related to the car's location, speed, type of road, hours and driving duration and transmit them every two minutes. The CNIL refused its authorisation for the processing of the data arguing that via the proposed system the insurance company would collect information about individual violations of the speed limit. Such processing would involve sensitive data and would infringe Article 9 of the French Data Protection Act, according to which private entities are not authorised to process data relating to criminal offences. In general, recording speed violations for the purpose of PAYD is regarded as excessive and illegitimate by CNIL. Speed information could be used, but should be based on average values. It is noted by the authors that it has been shown in various studies that speeding is one of the most important causes / circumstances of traffic accidents, which would provide a ground to use this parameter to differentiate premiums.

Other recommendations from [45] and [46] include:

- the subscriber should be fully informed about the processing of personal data before he is asked to consent to the data processing involved
- the policy holder should be given the option to withdraw his consent for the PAYD scheme and have the blackbox removed
- the data should be kept no longer than needed for calculation of the premium (possibly respecting a period for appeal)
- the communication between blackbox and data collection system should be provided with adequate confidentiality and integrity mechanisms
- central storage of data should be provided with adequate access control to avoid unauthorised disclosure
- further processing of the data e.g. to define personal user profiles would be illegitimate
- domain separation can be recommended to shield off vehicle usage details from the insurer. This is relatively easy to implement as the

insurer will likely involve a third party service provider to manage the blackboxes and perform data collection and premium calculations

- [46] recommends that European countries lay out clear legal rules which would specify how and under what circumstances judicial authorities can access PAYD data.
- [46] further recommends a 'thick client' approach, where the measured detailed data would be transformed into aggregated quantities that determine the premium. This approach is also recommended in [29]. It is noted by the author that decentralised processing imposes higher requirements on the integrity of processes and stored data inside the blackbox. Similar to road pricing, a detailed log may still be required for the user as a means to appeal against erroneous invoices of the insurer. It is conceivable that access to details on the OBU is only available for the user / vehicle keeper. PriPAYD can be considered as an example of such a Thick Client solution, see 2.2.1.4 and [82].

A concern specific concern raised by the UK information commissioner (ICO) is how the risk of on-going collection of data is managed when an insurance policy is lapsed or cancelled while the black box is still in place. Physical removal of the black box may not be a cost-effective approach. Possible solutions range from disabling the mobile data service to breaking the association with an identity which would require additional measures as well.

3.2.6.8. MAJOR THREATS AND DATA PROTECTION MEASURES

All defined threat areas are in principle relevant for PAYD:

- T1: Unauthorised access to personal data, by eavesdropping, unauthorised actions of staff, hacking etc.
- T2: Re-use of personal data beyond the legally defined purpose or beyond the scope of the consent of the data subject. This risk is ranked 'high', as the detailed data may have considerable value for other purposes.
- T3: Excessive processing, i.e. processing more personal data than required for the purpose. This risk is ranked high, as the controller may wish to seek for new indicators that have a higher predictive value of crash risk than the basic ones (distance, time, location).

Relevant measures are observed in the following areas:

- M3: data minimisation
- M4: domain separation
- M6: deletion immediately after initial processing
- M7: distributed processing
- M8: data subject control

3.2.7. SECTION SPEED CONTROL

3.2.7.1. BRIEF DESCRIPTION

Section control is a method of speed enforcement involving a series of cameras installed over a stretch of road. An image that contains the vehicle's number plate and corresponding timestamp are recorded for each vehicle as they enter and leave two points in the system (a section of road). The vehicle registration mark is extracted from each image by ANPR. On the basis of extracted vehicle registration marks, the entry and exit records are matched. The average speed is calculated as the fixed distance between the registration points divided by the time difference between the timestamps of the entry and exit record. In case the calculated speed exceeds the local speed limit, an enforcement record is created. To compensate for system inaccuracies and to increase public acceptance normally some margin is deducted from the measured average speed. Entities in charge of traffic enforcement and traffic safety interest groups emphasise the great advantages of this technology to enforce speed regulations:

- The costs per check are low, as the checks can be executed in a fully automated process.
- The effect on speed regulation compliance is impressive, due to a high chance of getting a fine. Moreover the effect is not restricted to one point on a highway but applies to the entire section. This also eliminates the potentially dangerous behaviour of motorists when suddenly aware of a conventional speed camera.
- Due to high user compliance, traffic safety is increased significantly. Speeding is one of the major causes of traffic accidents.
- When adequate speeds are set, the section control may also contribute to a higher throughput of the road.
- User acceptance of section speed control is believed to be higher than for conventional speed checks, as the user is aware of the check and an unintended short moment of speeding will not lead to a fine.

A good summary of section speed control and its effects is given in [47].

From a data protection perspective one element in this application is of specific concern. Whereas for conventional speed checks only data are collected of vehicles with speeds exceeding the local limit, section speed control collects data of all vehicles that enter the section. As the vehicle registration mark can be linked to the vehicle keeper, this is to be regarded as processing of personal data.

3.2.7.2. LEGAL FRAMEWORK

The legal basis for using the instrument of section speed control to enforce traffic speed limits is usually embedded in national road traffic legislation, i.e. LB1. The equipment used is generally subject to specific certification and calibration procedures.

The application falls outside the scope of the data protection directive, [4]. It seems sensible to apply the generic principles of data protection also to this case.

3.2.7.3. LEGAL BASIS FOR THE PROCESSING

Specific national legislation on methods and instruments of the police for traffic regulation enforcement.

3.2.7.4. TERMINOLOGY

No specific terminology.

3.2.7.5. HIGH-LEVEL APPLICATION ARCHITECTURE

Section control relies on detection of vehicle passages at, in general, two locations on one road section, relying on ANPR. The passages are collected at a central system or in a roadside unit.

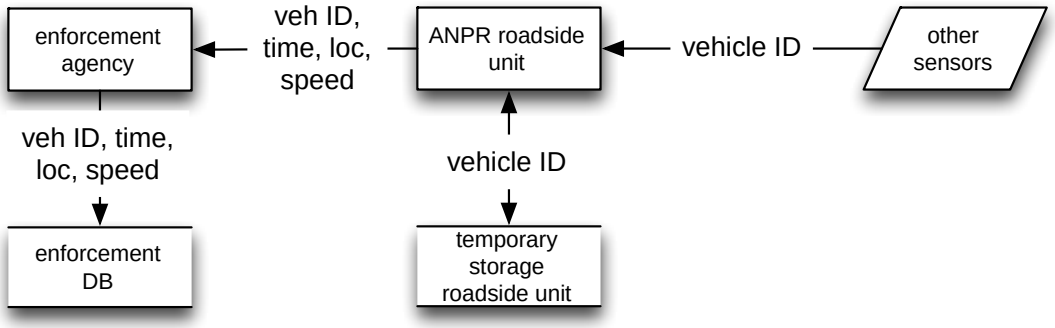


Figure 18 Global technical architecture of a speed section control system. Abbreviations used: veh ID=vehicle identification number, loc=geographic location.

3.2.7.6. CATEGORIES OF PERSONAL DATA INVOLVED

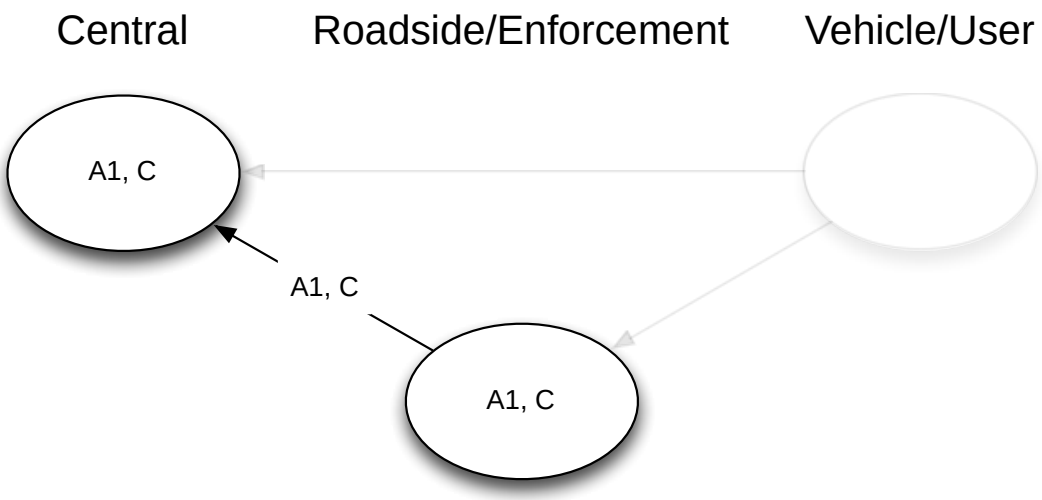


Figure 19 Global representation of the storage and exchange of personal data in the different domains of a section speed control system.

The processed data are classified as type:

- A1: Occasional single samples of position and time
- C: Details of driving behaviour (speed)

Also the special category C* is processed:

- C*: Driving behaviour that indicates a criminal offence. Such events are also reported to the central system.

It is noted that common events of speeding are 'ordinary' administrative violations. Only excessive speeding is generally regarded a criminal offence.

3.2.7.7. DISCUSSION

As mentioned above, this application falls outside the scope of the data protection directive, yet it is sensible to apply its general principles.

This would lead to the following 'guidelines':

- Complete passage records, as well as the images of the passing vehicle are to be deleted from the system in case that, and immediately after the speed measurement has indicated that the speed was below the threshold set for issuing a fine.
- The initial speed calculation shall be performed locally, i.e. by the roadside system, as soon as the vehicle passed the exit of the section.
- Adequate measures shall be taken to safeguard the confidentiality of passage records, images stored in the roadside equipment as well as on transmission of records relating to violations to the central equipment for follow-up.
- The collected data should not be used for any other purpose than speed regulation enforcement. This point seems important for public acceptance.

It is noted that requirements on authenticity and integrity of data are not listed as they are imposed by their use as legal evidence of a traffic violation.

3.2.7.8. MAJOR THREATS AND DATA PROTECTION MEASURES

The following threat area is deemed of specific importance to section speed control:

- T2: Re-use of personal data beyond the legally defined purpose.

An interesting example of such secondary use is a case at the Dutch Supreme Court. In this case, [48], stored images from ANPR police cameras should have been deleted (i.e. violation of police law) but were available and were used as evidence against the vehicle keeper in a serious criminal case. The court ruled that

the interest of prosecution should prevail over the infringement in the personal life caused by the disclosure of the traffic images.

The following types of measures are relevant to this application:

- M6: deletion immediately after initial processing
- M7: distributed processing

3.2.8. FLEET MONITORING

3.2.8.1. BRIEF DESCRIPTION

For the scope of this document, fleet monitoring is the use of GNSS/CN technology to monitor the location of vehicles or goods/persons transported. This may serve several purposes, including real-time fleet localisation, dynamic trip/resource planning, dynamic information to customers as to progress of deliveries or services, to keep detailed records of vehicle usage for maintenance, to register working hours / productivity details of personnel for calculation of wages or performance monitoring and anti-theft protection. It is noted that the use of fleet monitoring systems is quite common in organisations that own or operate fleets of vehicles, and where transport of people or goods is an important component of the business activities. This does not imply that fleet monitoring is always legitimate; the processor needs to fulfil the conditions and criteria for legitimate processing following the data protection directive.

Fleet monitoring is often applied in the following areas of business areas:

- Logistics, heavy goods transport
- Field service, e.g. maintenance of equipment or other services provided on location
- Postal and express delivery services
- Taxi's
- Public transport

3.2.8.2. LEGAL FRAMEWORK

No specific legal framework.

3.2.8.3. LEGAL BASIS FOR THE PROCESSING

The legal basis of this application is generally of type LB3, the protection of the legitimate interests of the processor. The processor is in this case usually the employer, the fleet owner or fleet operator (or a combination of these).

The legal basis may also be of type LB2, explicit consent of the data subject. It is noted that consent given by a data subject in the context of an employee-employer relationship cannot always be considered freely given. Therefore, LB3 seems the dominant ground for processing.

3.2.8.4. TERMINOLOGY

No specific terminology.

3.2.8.5. HIGH-LEVEL APPLICATION ARCHITECTURE

Fleet monitoring solutions in general relay real-time position data for multiple vehicles to a central system. Often manual input by the driver, and input data from other sensors, such as the cargo temperature, are also monitored and stored in the central system.

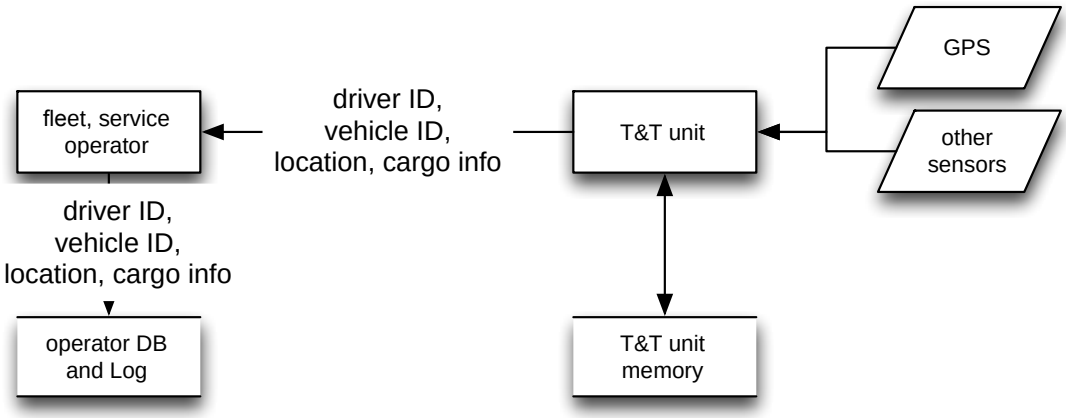


Figure 20 Global technical architecture of a fleet monitoring system. The exact implementation will vary between providers of the solution.

3.2.8.6. CATEGORIES OF PERSONAL DATA INVOLVED

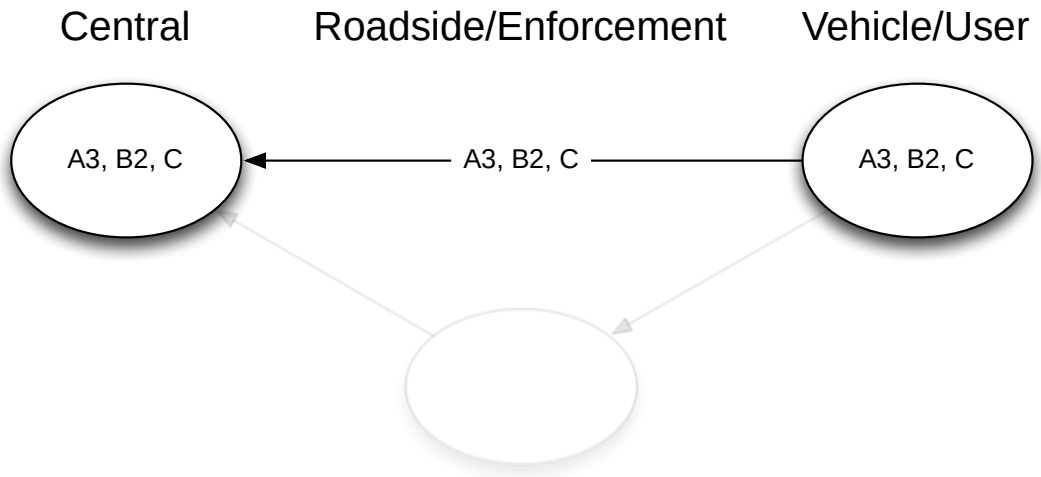


Figure 21 Global representation of the storage and exchange of personal data in the different domains of a fleet monitoring system. The exact implementation will vary between providers and fleet operators.

The type of data depends on the implementation. In general the following categories are processed:

- A3: Complete traces of the vehicle. In addition, a driver is often linked to the use of the vehicle.
- B2: Complete logs of trips
- C/C*: often also driving/vehicle characteristics are monitored. This may be done for purposes of vehicle maintenance management but also to 'encourage' good driver behaviour. It is not excluded that a criminal offence (excessive speeding) can be detected from the data.

3.2.8.7. DISCUSSION

As fleet monitoring is widely deployed, codes of practice are in place in several Member States. A good example is found in the guidelines of the Slovenian Information Commissioner, [38]. The guidelines have the broader scope of personal data protection in employer-employee relations, but specifically address the case of using GPS technology. This document states:

"The employer has no right to access employees' e-mails, control the use of work phone when the employee has the right to use it for private purposes as well, and has no right to track the movement of work vehicles with GPS technology, when the vehicles are also used for private purposes, etc. Case-law indicates that the employer cannot justify the control over privacy (especially communication privacy, i.e. confidentiality of all the forms of communication – post, telephone, e-mail) with the fact that the work means (the vehicle, telephone) are his/her property and hence he/she has the right to manage them."

This does not mean that fleet monitoring systems are never legitimate if the vehicle is used for private purposes as well. It does not mean either that processing of personal data is always allowed in case the vehicle is used only during work hours.

The document, [38], further states:

"The Commissioner's opinion is that the employer may have legitimate grounds for implementation of vehicle fleet tracking but he/she has to consider the use of such technology with reference to personal data protection. The employees have a legitimate right to a reasonable expectation of privacy within the work area, hence in the work vehicle, especially if the vehicle may be used for personal purposes outside of working hours. The Commissioner draws attention to the recent decision of the European Court of Human Rights in the Copland vs. United Kingdom case.

The Court extended the employee's right to privacy by adjudicating that the employer's breach of privacy was unjustified. Crucial for the decision was the fact that the employee had not been informed about when, and in what cases the employer may control the e-mails. The same principle must be applied in the case of GPS technology surveillance. The employee has to be informed in advance about when, and in what cases the employer may control the vehicle. Usually the use of work vehicles is defined specifically in internal acts of organizations (i.e. rules about vehicle fleet use). The Commissioner believes that use of any kind of vehicle tracking technology, including GPS, has to be defined specifically in an act like that. All the employees, or at least the ones who use the vehicles, have to be informed about the terms of use. The employer has to respect the principles of personal data protection and safeguard the employee's right to privacy when implementing vehicle tracking technology."

It is observed that the crucial element is the grounds the employer has for processing the data, the nature of the data and the question whether these data are really required for the purpose. As this is different from case to case, these guidelines (and similar ones in other countries) remain rather generic. In general, there are often reasonable grounds out of business interests to improve planning and management of key resources through some form of fleet monitoring. Still, this does not imply there is a legitimate ground for all possible processing of monitoring data. For each type of data/processing there should be a clear relation to the business purpose, the processing should be proportional and the goal should not reasonably be achievable with means that are less invasive to privacy. In particular, data that relate to the (permitted) use of company vehicles outside working hours shall not be processed – unless specific sufficient grounds exist for such processing. This can e.g. be achieved by a user interface to the device where the driver can indicate whether a trip has a business or private character and where no location or detailed trip information is collected in case the trip is indicated 'private'. Another solution is to apply fixed or adjustable time windows that correspond to working hours for collection of fleet monitoring data.

Another important condition is that the employees are fully informed about the ways the technology is used, the ways it works, the purpose of its implementation, and the situations in which the acquired data may be used. Additionally, it has to be clear that the data may only be used for purposes and in situations that are clearly defined in advance. Finally, adequate measures to protect the personal data collected should be in place. It is required that all these aspects are laid down in writing in a company regulation.

It is noted that fleet monitoring systems are widely accepted in certain sectors (mostly those where transport is the core activity) but cause more discussion in others, especially those where vehicles are frequently used for private purposes. In all cases a careful approach to introduction, where the point of view of employees

is also taken into account, pays off as a system that is not accepted by those primarily concerned may also fail to deliver the objectives.

We summarize the good practices as follows:

- The legitimacy of the grounds for the processing are assessed for each specific case. It is the responsibility of the processor to take care of such an assessment.
- Companies should describe the specific purposes of the fleet monitoring, the data involved, the conditions/situations in which they are collected and the measures to protect the data in a company document that is available to all employees.
- Companies should discuss the details of a fleet monitoring service with employees or their representatives, prior to deployment.
- Specific attention should be paid to measures to avoid the processing of personal data for the use of vehicles outside working hours.

3.2.8.8. MAJOR THREATS AND DATA PROTECTION MEASURES

For fleet monitoring T3 (excessive processing) is of particular concern, but there is also a clear risk of T1 (eavesdropping, hacking) and T2 (Re-use of personal data beyond the legally defined purpose). T3 is considered 'high', as – once the system is deployed (usually within a company) – it is often relatively easy to change operational parameters, and supervision of data protection rules, while management of user access rights can be quite limited in an environment where this is not core business.

Most relevant measures to enhance data protection in this area are:

- M3: data minimisation
- M4: domain separation
- M8: data subject control

3.2.9. TRAFFIC DATA COLLECTION

3.2.9.1. BRIEF DESCRIPTION

Traditional techniques for traffic data collection use stationary sensors (mounted at the roadside or on gantries above the road) that measure vehicle flux and/or speed without any possible identification of the vehicle. Such systems are not further discussed here, as they pose no threat to privacy.

In the last two decades, powerful new methods have emerged that require more attention from a personal data protection point of view. The following types can be distinguished:

- *I: Floating car / vehicle data*: the vehicle is used as a 'probe' to measure the traffic situation with a device that determines its position and speed using GNSS, and forwards the information through a mobile network. This type of data collection normally requires a specific service to which

a user has to subscribe, and requires a specific device which may also serve other purposes (e.g. route guidance). A detailed privacy-centred analysis of this application can be found in the Privacy Issue Analysis of the PRECIOSA project, see [43].

- *II: Floating cellular data*: a cellular phone or data device installed in the vehicle or carried by the driver or occupants of the vehicle is localised in the mobile network. Subsequent localisations of the same device allow calculation of traffic speed. As current mobile networks do not allow a localisation with high accuracy, advanced statistical methods are applied. The obvious advantage of this approach is that the 'probes' do not need to subscribe or to use dedicated equipment: a switched-on handheld is sufficient. A drawback is that significant investment in the base station network of the mobile operator is needed to extract the operational data required for traffic measurement.
- *III: Roadside-based travel time measurement.* In this case individual vehicles are detected at different locations in a road network. By comparing passage times, average speeds can be calculated that are specific for the given route and time. With data from large volumes of vehicles and a number of observation points on strategic roads/nodes, rather accurate travel times can be calculated for the entire network. This approach requires that a passage of a vehicle at one point of observation can be linked to its passage at the next. Some form of identification is therefore required. Most common is the use of ANPR cameras for this purpose. More recently, also sensors that use the Bluetooth ID of handhelds are used.

3.2.9.2. LEGAL FRAMEWORK

For type II data collection systems (floating cellular data), type II, data from electronic communication service providers are used. Consequently, the privacy directive for the electronic communications sector [9], also applies.

3.2.9.3. LEGAL BASIS FOR THE PROCESSING

The legal basis for the processing for type I (floating car data based on GPS) is LB2: explicit consent of the user.

All personal data processing involved in type II should be based on [9]. All resulting data that are processed outside the mobile operator's domain are fully anonymised.

For type III (roadside based) it seems that LB3 should apply: the legitimate interest of a traffic information service provider or road authority to provide traffic information or monitor road status in the public interest, prevailing over fundamental rights to privacy of the road user. It is noted that in any case the privacy infringement should be minimal to satisfy this criterion from the directive.

3.2.9.4. TERMINOLOGY

Floating Car Data: method to calculate travel times from locations and time stamps from individual vehicles on a road network.

Floating Cellular Data: method to calculate travel times from position information of handhelds available in the core network of the mobile operator.

3.2.9.5. HIGH-LEVEL APPLICATION ARCHITECTURE

The different traffic data collection technologies require different system architectures.

Systems based on floating vehicle data rely on on-board units that collect sensory input to determine the vehicle's travel time and speed for specific road links. In general the on-board units are thick clients that will determine the relevance of information in order to limit the amount of data that is transmitted to the central system. This implies personal data is, at least temporarily, stored on the in-vehicle device. Most data is transmitted anonymously to the central system.

The central system collects information from many probe vehicles, to compose a complete picture of the traffic situation in an area.

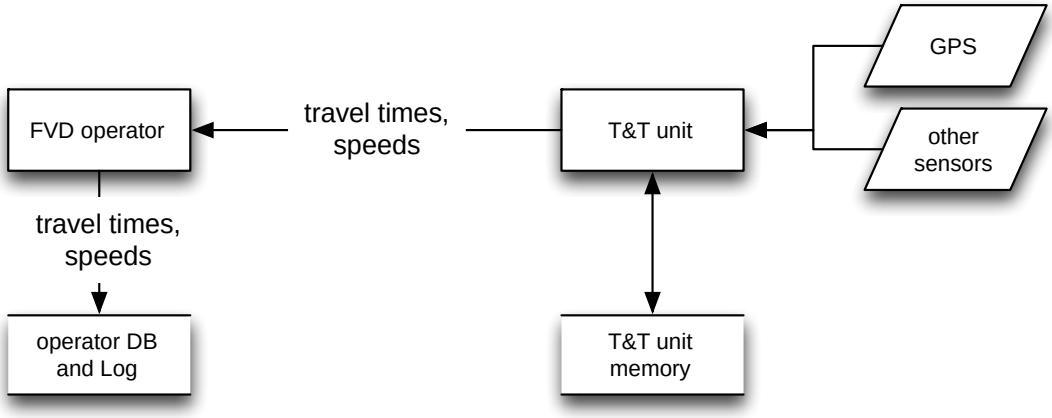


Figure 22 Global technical architecture of a traffic data collection system based on floating vehicle data. The exact implementation will vary between providers.

Traffic data collection based on floating cellular data, retrieve data on the positions of mobile phones from central systems of a mobile telecom operator. These position data are then used in the central system of the traffic information provider to derive travel times and traffic speeds for the transport network.

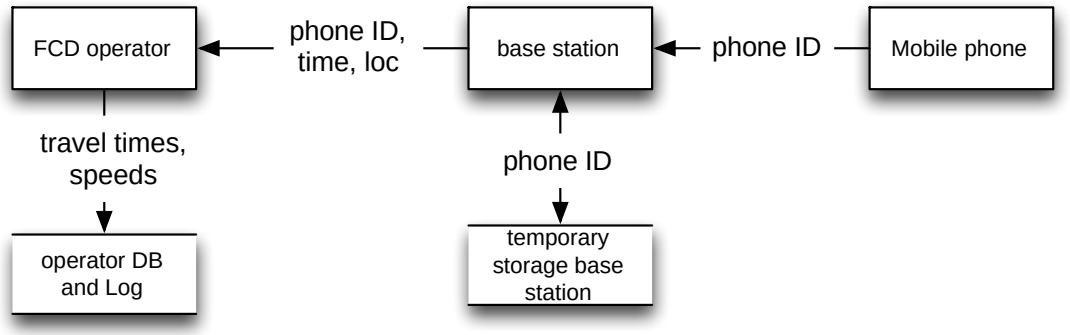


Figure 23 Global technical architecture of a traffic data collection system based on floating cellular data. The exact implementation will vary between providers. Abbreviations used: Phone ID=phone identification number, loc=geographic location.

Systems that rely on roadside equipment to collect traffic data again use a more straightforward architecture. The roadside equipment may rely on different technologies, e.g. detection of passing Bluetooth devices, or ANPR. By matching passing vehicles at different locations, travel times and traffic speeds can be determined. In general measurement data is immediately relayed to a central system. The central system uses the data to generate traffic information.

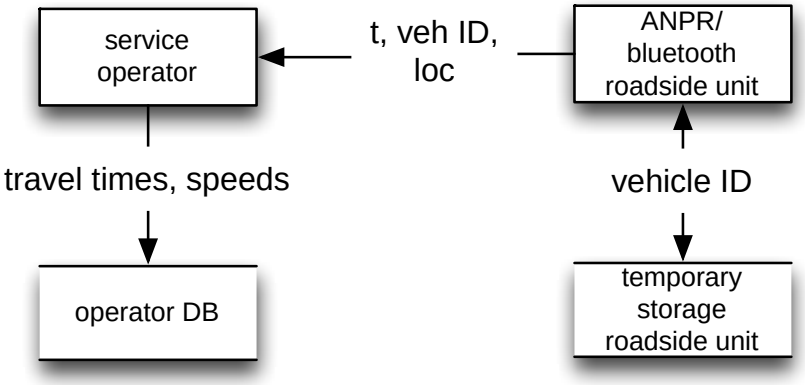


Figure 24 Global technical architecture of a traffic data collection system based on roadside equipment. The exact implementation will vary between providers. Abbreviations used: t=timestamp or period, veh ID=vehicle identification number, loc=geographic location.

3.2.9.6. CATEGORIES OF PERSONAL DATA INVOLVED

For type I the type of personal data processed is classified as:

- A3: Complete mobility patterns of the vehicle are processed in the in-vehicle unit. The information that is transmitted to the central system is normally aggregated to information on average speeds on specific road

links. At the central system, traceability can be reduced by using different pseudonyms for parts of journeys, i.e. in such a way that it is no longer possible to reveal complete mobility patterns of an individual vehicle. The centrally processed information therefore classifies as A2.

- C: Speed information is also processed.

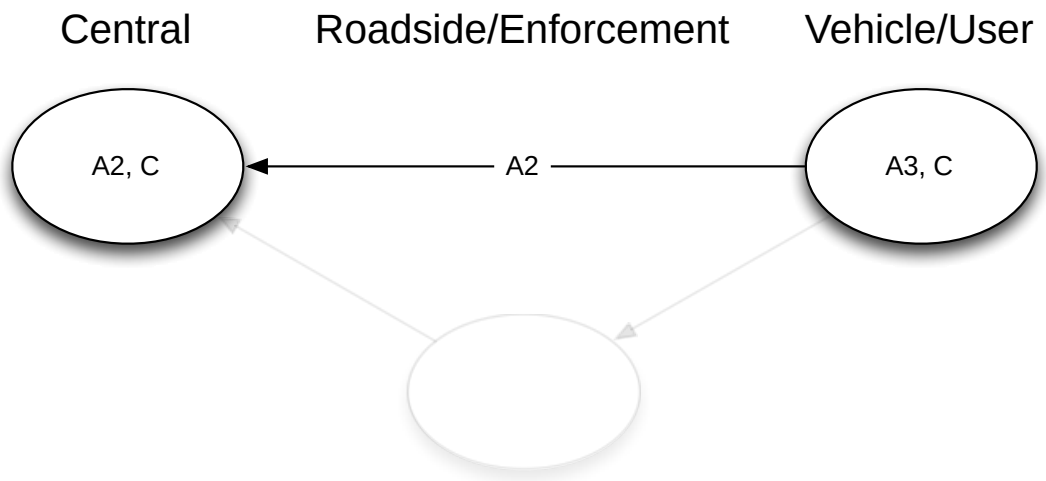


Figure 25 Global representation of the storage and exchange of personal data in the different domains of a traffic data collection system based on floating vehicle data. The exact implementation will vary between providers.

For type II, the classification is slightly different from the one for type I:

- A2: In the cellular communications network, handhelds are traced with an almost complete geographical coverage. However, the accuracy of position information is low and does not reveal complete mobility patterns. It is also noted that part of the processing takes place inside the de-central nodes of the network which do not monitor the entire network. The information processed centrally is further aggregated and does not support (full) traceability of individual devices.
- C: Speed information is also processed.

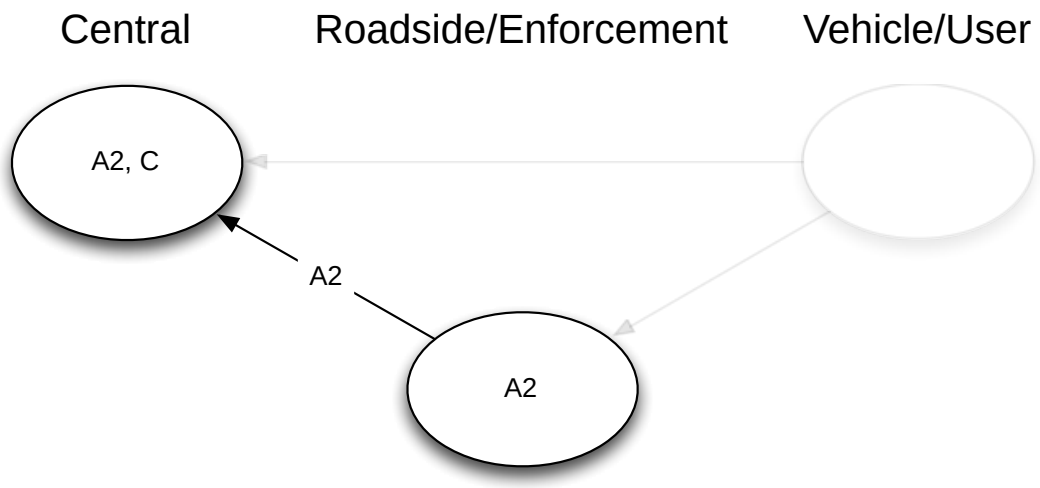


Figure 26 Global representation of the storage and exchange of personal data in the different domains of a traffic data collection system based on floating cellular data. The exact implementation will vary between providers.

Type III normally involves:

- A1: Occasional samples of position and time.
- C: Derived speed information is processed centrally.

It is noted that with a dense and extended network of observation stations the classification could become A2 or even A3.

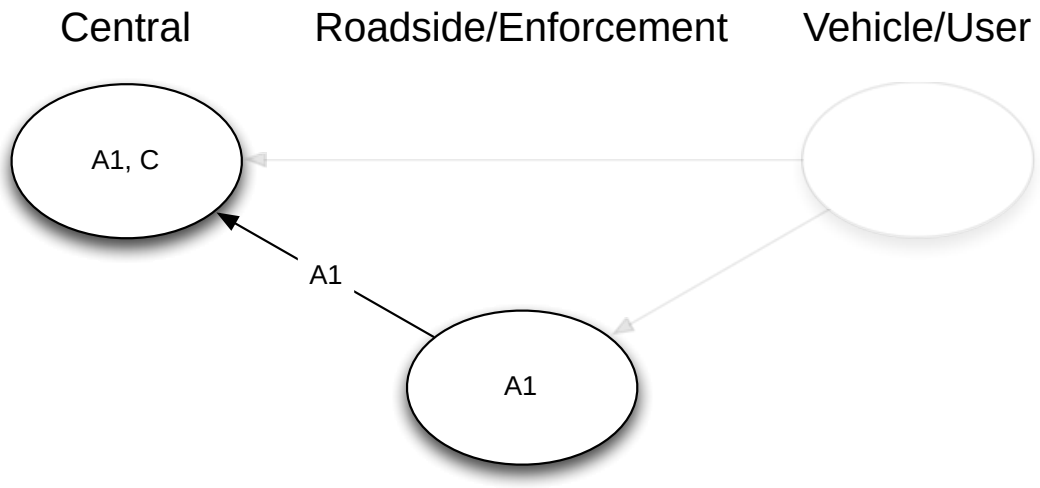


Figure 27 Global representation of the storage and exchange of personal data in the different domains of a traffic data collection system based on roadside equipment. The exact implementation will vary between providers.

3.2.9.7. DISCUSSION

Type I: GNSS-based floating vehicle data.

This type of data collection normally involves consent of the person who subscribes to the service (most often the user or the owner of the vehicle). For cost reasons, GNSS-based FVD is hardly ever a standalone service. The following common examples may illustrate how FVD is combined with another service:

- Subscribers to advanced route guidance services receive high quality real-time traffic information and dynamic routing advice. At the same time their device is used as probe and regularly sends its position to the data collection server. Subscribing to the route guidance service requires accepting that your position data are used to improve the service.
- Fleet management service providers already process detailed tracking information on individual vehicles. It is relatively easy to further process these data in an anonymous form for traffic information purposes.

In the first case it is of key importance that the user gives his informed and explicit consent to the collection and processing of his movement data. A typical issue is that some form of agreement is in place containing conditions for use of the service, which also addresses the use of the data for traffic data collection. The consent given is not explicit, and information on what data are exactly processed and for what purpose is often too limited. Illustrative is the dispute between TomTom and the Dutch national data protection supervisor, see [39]. It concerns connected devices that send position information in real time, as well as non-connected devices that store position information which is forwarded to the service provider's back-office at the moment the device is connected to an internet PC to receive updates.

For Floating Vehicle Data the question whether a fully anonymous method is feasible is relevant. This is a hard problem that is not solved by simply removing or skipping any fixed source ID (subscriber ID, device ID, MAC address) from the messages. Message integrity/authenticity mechanisms that are required may also render the origin identifiable. And finally, if multiple positions and timestamps can be connected to one source, this may also enable identification with a certain probability. Several scientific papers report partial solutions to the problem, see [40] and [41]. Best effort algorithms using pseudonymisation have been elaborated which can guarantee a maximum 'time-to-confusion' for all vehicles involved, for a given accuracy of tracking data. It is concluded that from a theoretical point of view, the problem of fully anonymous Floating Vehicle Data is unsolved, although methods exist to significantly reduce the chances of identifying individual vehicles/drivers from given sets of Floating Vehicle Data. It is not expected that such methods are applied in today's commercial services, but dedicated investigation would be required to verify this. It is further noted that in cases where Floating Vehicle Data is a spin-off of another application that requires individual vehicles to be monitored anyway (e.g. Fleet Monitoring), the option of anonymous data collection does not add value.

Assuming that the raw collected FVD-data are to be regarded personal data, the straightforward 'rules' from the data protection directive lead to the following recommendations:

- Make sure the data subject gives his explicit and informed consent, as discussed above.
- Transform the centrally collected data to suitable basic traffic data (e.g. time series of link travel times) that do not relate to individual vehicles and hence do not qualify as personal data, at the earliest possible stage.
- Delete the raw FVD data immediately after processing and in any case within 24 hours.
- Take adequate security measures to protect the FVD messages against disclosure to unauthorised parties.
- Where FVD data are stored on the in-vehicle device prior to sending the data to a central server, the data should be deleted from the device after the messages have been sent successfully (unless there would be an explicit wish and action by the user to keep local records for a longer period, for other personal purposes).

Similar, more generic recommendations can be found in the basic principles for probe vehicles formulated by ISO, see [42].

Type II: Floating Cellular Data

A number of recommendations concerning the use localisation data is available, see 2.2.2. These recommendations all address the situation where localisation data are processed on request or with explicit consent of the data subject, see e.g. [26]. However, the key advantage of using cellular data is that no new contracts (and devices) would have to be issued with individual 'probes'. The data are derived from operational information from a cellular network. Still, if this would involve the processing of personal data for other purposes than providing the communication service, without explicit consent of the data subject, the processing would likely be illegitimate. It therefore seems required, that the mobile network operational data that are processed to derive road traffic data do not allow identification of individual users. Whether this condition is completely satisfied in operational systems is not known.

A weaker but pragmatic requirement is that the third party using the (pre-processed) floating cellular data will not receive any data that can be linked to identifiable users. In this case the mobile operator should also motivate that the preparation of road traffic information does not lead to a situation of excessive processing of personal data in relation to the provisioning of the communication service.

Type III: Roadside based travel time measurement

Processing of personal data in this case has to be marginal, as there is no consent of the data subject involved nor a legal obligation for such processing. The privacy impact can be marginalised by the following measures, which are reported to be applied in practice:

- The received or observed unique ID (e.g. optically registered vehicle registration mark or Bluetooth MAC ID), is immediately transformed by a one-way function into a pseudo ID which is not globally unique but can be matched with other observations of the same vehicle with high reliability within definable time and geographic constraints. It is noted that for travel time analysis, 100% matching is not required, and external rules can be applied to filter out impossible matches.
- The transformation mentioned above is carried out in real-time in the observation device, preferably in hardware with increased security provisions. The unique ID is not kept.
- The position+timestamp+pseudo-ID data are discarded after their processing into traffic data.

3.2.9.8. MAJOR THREATS AND DATA PROTECTION MEASURES

Type 1 (GNSS FVD)

All threat areas are important:

- T1: Unauthorised access to personal data
- T2: Re-use of personal data beyond the legally defined purpose or beyond the scope of the consent of the data subject. This threat is ranked ‘high’, as these detailed data may have considerable value for other purposes.
- T3: Excessive processing, i.e. processing more personal data than required for the purpose. This risk is also ranked ‘high’, for the same reason as T2.

Relevant measures are in the following areas:

- M1: anonymisation
- M2: pseudonymisation
- M4: domain separation
- M5: user consent mechanisms

Type 2 (Floating Celllular)

The following threat area seems of specific importance:

- T2: Re-use of personal data beyond the legally defined purpose or beyond the scope of the consent of the data subject.

Relevant measures are in the following areas:

- M1: anonymisation
- M2: pseudonymisation
- M4: domain separation

Type 3 (Roadside Based)

The following threat area seems of specific importance:

- T2: Re-use of personal data beyond the defined purpose. It is imaginable that the data would be of value for other (public) purposes such as speed limit enforcement, vehicle taxation compliance checking or criminal investigation.
- T3: Excessive processing, i.e. processing more personal data than required for the purpose.

Relevant measures are in the following areas:

- M1: anonymisation
- M3: data minimisation
- M6: deletion immediately after initial processing

3.2.10. COOPERATIVE SYSTEMS

3.2.10.1. BRIEF DESCRIPTION

Cooperative systems are a special category as it cannot be regarded as a single application but an unlimited variety of applications that have in common that communication with other vehicles and/or roadside systems through ad-hoc wireless networks is essential. Most applications we can imagine today are in the area of traffic safety or traffic management.

Another reason that cooperative systems stand out is the stage of development: whereas other applications discussed in this study have numerous deployments, cooperative technology has so far only been demonstrated on test sites. Standards are essential in this area, as any vehicle should be able to communicate with any other vehicle as well as with roadside systems in various countries. Although good progress is made so far, standardisation is still on-going.

It is expected that vehicle to vehicle (V2V) applications will generally have a faster rate of deployment than applications that require interaction between vehicle and infrastructure (V2I). This is due to the fact that full deployment of cooperative roadside infrastructure requires considerable investment from a great number of road operators, whereas integration of cooperative technology in new vehicle models is likely to start within a few years time. Standardisation efforts assume that cooperative awareness, longitudinal collision risk warning but also intersection risk warning – which is a V2I application – are 'early' cooperative applications, see 2.3.3.

3.2.10.2. LEGAL FRAMEWORK

No specific legal framework.

3.2.10.3. LEGAL BASIS FOR THE PROCESSING

At least for the next few years, the legal basis is expected to be LB2, explicit informed consent of the user. On the longer term, it is likely that certain applications will become mandatory in the interest of traffic safety, implying LB1. It is noted that, as a first step, such an obligation is expected to apply to new vehicles only.

3.2.10.4. TERMINOLOGY

3.2.10.5. HIGH-LEVEL APPLICATION ARCHITECTURE

Co-operative systems rely on a complex interaction between vehicles, between vehicles and roadside equipment, between vehicles and one (or more) central system, and between roadside equipment and central system. Different deployment options are possible, resulting in different possible architectures. The diagram below presents the most common approach.

The on-board unit collects sensor information in the vehicle, derives information from the sensor data, and exchanges relevant information with other vehicles in the area, roadside equipment, or a central system.

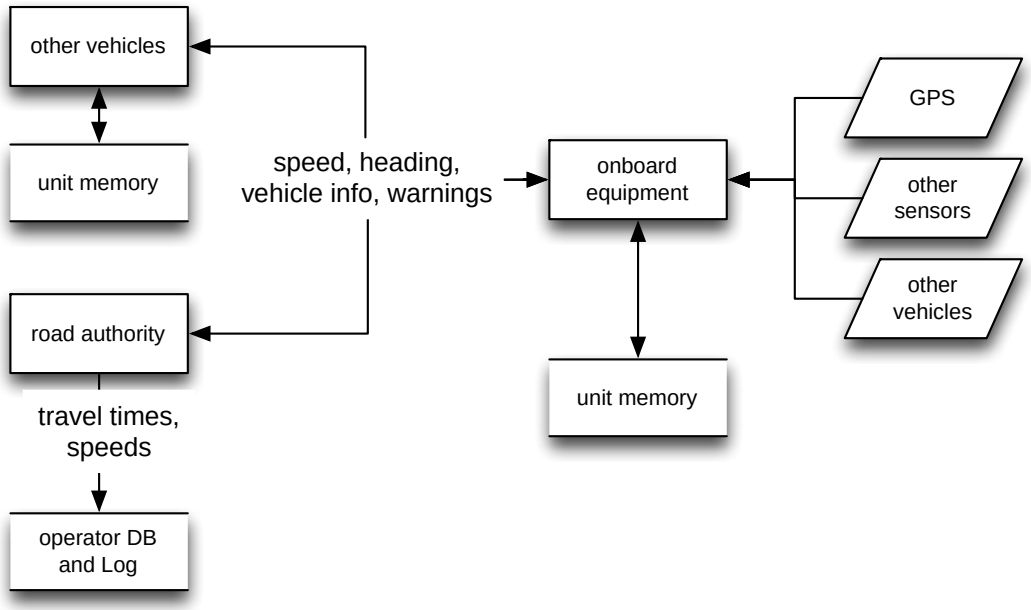


Figure 28 Global technical architecture for a co-operative system. The exact implementation will vary between schemes.

3.2.10.6. CATEGORIES OF PERSONAL DATA INVOLVED

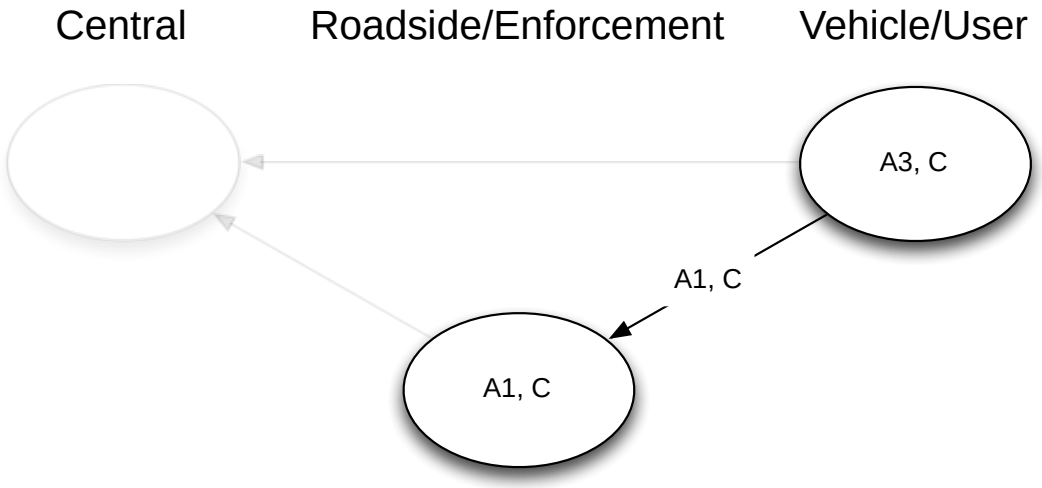


Figure 29 Global representation of the storage and exchange of personal data in the different domains of a co-operative system.

It is not unlikely that some of the data processed locally by vehicles and roadside infrastructure will be collected centrally for purposes of traffic management and traffic information. The nature and detail of such data is currently unclear. For simplicity only the primary decentralised cooperative applications are assessed.

- A1: Occasional single samples of position and time. Assuming that a vehicle will communicate with a set of other vehicles that changes all the time, and that the cooperative roadside systems operate locally and autonomously, there is usually no data processed that allows reconstruction of complete traces of a vehicle. It should be noted that if the broadcasted or periodically sent messages from a vehicle can be received continuously, or concentrated centrally from a network of receivers, the data would be classified as A3.
- A3: the in-car system will continuously process time-stamped positions of the vehicle in which it is installed.
- C: Details of driving behaviour. In particular speed is an important parameter for safety applications. In addition, information from other sensors in the vehicle may be sent to other vehicles or the roadside. It is imaginable that information indicating (criminal) offences is also processed.

3.2.10.7. DISCUSSION

Probably because cooperative applications still have some distance from actual deployment, it has not been addressed yet in guidelines or opinions from data protection supervisors. It is noted that privacy and security aspects are key

success factors and are of prime concern to the industry and the standardisation work groups involved.

ETSI produced a comprehensive threat and vulnerability analysis both on the level of a basic set of applications as on common messages, see [53]. Various (cryptographic) measures are elaborated to implement formulated detailed requirements on confidentiality, integrity and authenticity of messages/data. See also section 2.3.3. It is not within the scope of this document to address these requirements in detail. The following high-level observations and recommendations seem valid:

- In the initial stages of deployment, the use of cooperative applications should be based on explicit and informed consent. This consent should allow opt-out of all cooperative interactions, and further be specific for distinguished applications.
- For the exchange of messages and management of the ad-hoc networks short-lived pseudonyms should be used to avoid traceability of individual vehicles. It is noted that this requirement, combined with communication needs and requirements on authenticity and integrity of data that are safety-critical, leads to technical/economical issues that have not been solved completely as of today.
- Exchanged data relating to an individual vehicle, its environment or the driver shall be minimised in view of the applications used / consented to.
- Where data relating to individual and identifiable vehicles are processed (either by systems in other vehicles or in the cooperative roadside infrastructure), these data should be deleted immediately after they are no longer needed for the specified purpose. This would not necessarily apply to aggregated/statistical data that can be derived from the raw data exchanged if they do not include any information that can be related to an individual vehicle.

The PRECIOSA project made an interesting contribution to elaborating a Privacy by Design process suitable for the environment where development of cooperative systems takes place, see 2.4.2. The authors note that several issues have to be further elaborated before the approach could be used in a commercial development process, but it seems a promising basis. A major challenge would be to have such an approach truly adopted by the industry.

3.2.10.8. MAJOR THREATS AND DATA PROTECTION MEASURES

The following threats are of specific relevance to cooperative systems.

- T1: Unauthorised access to personal data, e.g. by eavesdropping. This is due to the nature of the application, as certain data are continuously broadcasted and can be received by any entity within range. The risk is therefore ranked ‘high’.

- T2: Re-use of personal data beyond the legally defined purpose or beyond the scope of the consent of the data subject. This risk is also ranked 'high' for the same reason as above: there is no control over the receivers of basic information exchanged between vehicles and with the roadside cooperative infrastructure.

The following types of measures are of specific importance for cooperative applications and technology:

- M2: pseudonymisation
- M3: data minimisation
- M5: user consent mechanisms
- M6: deletion immediately after initial processing
- M7: distributed processing

3.3. Overview of Results

This section provides an overview of the results collected in the application assessment. It provides insight into general similarities and differences between the various applications in terms of the use of personal data, legislation, system architecture, and privacy threats.

The table below lists per application: the legal basis, and the types of personal data that are processed in the different domains of the value chain.

Table 2 Overview per application of the legal basis, and the types of personal data and their storage location in the value chain. The colours represent an indication of the sensitivity of the data: yellow = low, red = high, orange = intermediate. Note that the information types (A1, B2 etc.) are always assigned the same colour.

			Type of information per domain																				
Application		**Legal Basis**	**Central system**							**Roadside/enforce.**							**Vehicle/user device**						
Nr	**Name**		**A1**	**A2**	**A3**	**B1**	**B2**	**C**	**C***	**A1**	**A2**	**A3**	**B1**	**B2**	**C**	**C***	**A1**	**A2**	**A3**	**B1**	**B2**	**C**	**C***
1	Digital tachograph	LB1																					
2	eCall	LB1 (LB2)																					
3	Road user charging																						
3a	RUC DSRC	LB1-3																					
3b	RUC ANPR	LB1-3																					
3c	RUC GNSS	LB1-3																					
4	eTicketing public transport	LB2-3																					
5	Parking payment services																						
5a	Online parking payment services	LB2																					
5b	TVM parking payment services	LB3																					
6	PAYD insurance	LB2																					
7		LB1																					
8	Fleet monitoring	LB3 (LB2)																					
9	Traffic data collection																						
9a	FVD traffic data collection	LB2																					
9b	FCD traffic data collection	LB3																					
9c	Roadside traffic data collection	LB3																					
10	Cooperative systems	LB2 (LB1)																					

The table below provides an overview of the legal basis and threat type for all applications. It shows that the legal basis does not determine the threat level. The threat level is determined by a combination of type of data that is collected, and to what extent personal data is centralised.

Table 3 Overview of the legal basis and threat type for all applications.

Application Nr	Application Name	Legal Basis	Threat type T1	T2	T3
1	Digital tachograph	LB1	Low	Low	Medium
2	eCall	LB1 (LB2)	Low	Low	Medium
3	Road user charging				
3a	RUC DSRC	LB1-3	Medium	Medium	Medium
3b	RUC ANPR	LB1-3	Medium	Medium	Medium
3c	RUC GNSS	LB1-3	Medium	High	High
4	eTicketing	LB2-3	Medium	High	High
5	Parking payment				
5a	Online parking	LB2	Low	Medium	Low
5b	TVM parking	LB3	Low	Medium	Low
6	PAYD insurance	LB2	Medium	High	High
7	Section speed control	LB1	Low	Medium	Low
8	Fleet monitoring	LB3 (LB2)	Medium	Medium	High
9	Traffic data collection				
9a	FVD collection	LB2	Medium	High	High
9b	FCD collection	LB3	Low	Medium	Low
9c	Roadside collection	LB3	Low	Medium	Medium
10	Cooperative systems	LB2 (LB1)	High	High	Medium

Explanation of codes:

LB1	processing is necessary for compliance with a legal obligation originating from national or EU legislation (Art. 7, clause c)
LB2	the data subject has given explicit consent for the processing of his personal data, mostly in the context of using of a voluntary service
LB3	processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection
T1	Unauthorised access to personal data, by eavesdropping, unauthorised actions of staff, hacking etc
T2	Re-use of personal data beyond the legally defined purpose or beyond the scope of the consent of the data subject
T3	Excessive processing, i.e. processing more personal data than required for the purpose.

The table below summarises the possible privacy enhancing measures.

Table 4 Overview of possible privacy enhancing measures per application.

Application		Importance privacy enhancing measures							
Nr	Name	M1	M2	M3	M4	M5	M6	M7	M8
1	Digital tachograph			■	■			■	
2	eCall			■		■			
3	Road user charging								
3a	RUC DSRC			■	■				
3b	RUC ANPR			■	■				
3c	RUC GNSS			■	■			■	■
4	eTicketing public transport	■			■	■			
5	Parking payment services								
5a	Online parking payment services				■		■		
5b	TVM parking payment services				■		■		
6	PAYD insurance			■	■		■	■	■
7	Section speed control						■	■	
8	Fleet monitoring			■					■
9	Traffic data collection								
9a	FVD traffic data collection	■	■		■	■			
9b	FCD traffic data collection	■	■		■				
9c	Roadside traffic data collection	■		■			■		
10	Cooperative systems		■	■		■	■	■	

Explanation:
M1 – anonymisation, i.e. data are no longer traceable to a natural person or vehicle
M2 – pseudonymisation, i.e. traceability is made difficult or strongly reduced by using temporary ID's
M3 - data minimisation, i.e. minimising the set of data to what is strictly needed for the purpose.
M4 - domain separation, i.e. the detailed usage or behaviour related data are processed in a separate domain, where user identification information (e.g. name, address, number plate) is not accessible. The other domain processes the identification information but only receives usage data on a high level of aggregation, as far as needed to bill or inform the user/client.
M5 - user consent mechanisms, i.e. mechanisms to provide the user with more control and awareness what personal data are processed for what purpose. This may e.g. involve user settings that certain information is never to be sent, other information always allowed for certain applications/destinations, and situations where a confirmation dialogue is presented.
M6 - deletion immediately after initial processing
M7 - distributed processing, i.e. the processing of the most detailed (and mostly most sensitive) usage/behaviour data is done locally , e.g. on the mobile device or in-car platform. Only the results needed for the central process (e.g. for billing) are transferred to a central system.
M8 - data subject control, i.e. the user is able to control the detailed personal data that is stored. He may delete data partly or completely, and decides whether or not to submit the data e.g. to substantiate a claim or appeal. This approach is sometimes applicable when the detailed data are not needed in the primary process, but are solely required for convenience and/or legal position of the user/data subject.

4. Measures and recommendations

4.1. Identification of areas of concern or potential improvement

4.1.1. ISSUES FROM THE PERSPECTIVE OF THE INDIVIDUAL

For many people privacy is a serious concern in a society where ever more data are processed and where not only fixed computers but also handheld devices, in-vehicle systems and household appliances are becoming more and more interconnected. Of course these developments bring clear benefits to the user: new possibilities, increased comfort and efficiency. Still people wish to understand what data concerning them are processed by whom and for what purpose, and have some control over it.

Mobility and transport is one of the areas that is strongly affected by new developments in ICT. The following issues are important from the perspective of the individual:

1. It is gradually becoming more and more difficult to move from one place to another without data being collected somewhere concerning this movement, be it by mobile networks, in-vehicle systems, electronic ticketing or parking payment systems or cameras. Although there are options to avoid participation / registration by most of such systems; in practice travelling without leaving traces is slowly becoming the exception rather than the rule.
2. Unambiguous and informed consent is still the legal basis for many ITS (and other) services. How the process of acquiring 'legally valid' consent should be facilitated by controllers has been addressed in a number of publications [67] [25] [26]. And although following these recommendations will certainly improve the situation for distinct applications, it will not fully compensate for the fact that a real understanding of all processing of one's personal data and its possible consequences is getting out of reach for more and more people.

4.1.2. ISSUES FROM THE PERSPECTIVE OF THE PRIVATE SECTOR

Few stakeholders in the EU will disagree that privacy is a fundamental human right and deserves adequate protection. The principles of personal data protection as laid down in the directive, [4], and its national implementations, have also proven to be stable and are not often disputed. However, the data protection legislation is essentially principle-based and does not provide a clear and simple set of rules for controllers and processors to be followed in order to be compliant. When it comes to practical detail of how personal data protection is to be provided, and to what extent the interest of personal data protection can be balanced against other

interests, there are diverging opinions. In practice, verdicts and decisions of data protection supervisors are the measure of how the law is to be interpreted. Such directions can be challenged by appealing to a court of justice – yet this happens only in rare cases. Consequently, the data protection supervisors have a key role in determining what is to be done/avoided regarding data protection. Taking this for a fact, the following criticism is heard from the side of the private sector:

1. It is not (sufficiently) clear what is to be done to meet data protection requirements for new products/services. Data protection authorities - whether for reasons of scarce resources, to avoid incompatible roles, not to be constrained in a later ruling or a combination of these - tend to be withholding when asked for advice on new systems and services that process personal data. Clear opinions are provided only when the service is already in an advanced stage of development - or already in operation - and the cost to change is considerable.
2. It is felt that data protection supervisors' opinions on data protection are sometimes extreme, i.e. more reflecting a privacy activists' position than following from a neutral interpretation of the law, balancing all the interests involved. This would apply to e.g. applying the definitions of '(sensitive) personal data' or 'excessive processing' and when balancing 'legitimate interests of the processor' against the interest of a minimal processing of personal data.
3. It is felt that the imposed requirements or solutions are not always balanced to the actual privacy risks involved in specific cases and that reasonable alternatives are excluded.
4. It is felt that data protection supervisors have a strong legal focus and insufficient eye for impact on / possibilities of IT and operations.

4.1.3. ISSUES FROM A LEGISLATOR'S PERSPECTIVE

As was mentioned in 4.1.1, privacy / personal data protection legislation is principle-based. This will not change with the adoption of the proposed new EU legal framework for data protection, [18] [19]. Considering the rapid developments in ICT, mobility and society, and the timelines of EU and national legislation processes, it seems a fact of life that such legislation will never be able to provide concrete rules for data protection on specific ITS applications or risk to be out-dated at the moment it enters into force.

The proposed regulation [18] leaves opportunity for the EC to further legislate in distinct aspects. It remains to be seen if this instrument will be available and effective to impose detailed rules for ITS applications.

4.1.4. ISSUES FROM A DATA PROTECTION SUPERVISOR'S PERSPECTIVE

From the responses to a questionnaire that was sent to the EU national data protection supervisors, it can be concluded that the priority of issues experienced differs from country to country, yet the following issues were recognised by a number of respondents:

1. In the development of new (ITS) technologies and applications the opportunity to adopt a true Privacy by Design approach (or a Privacy Enhancing Architecture) is – at least occasionally – missed. At the point a non-compliance is detected, fundamental changes are usually difficult and costly. Also in the process of standardisation, where industries work together to define the 'building blocks' of interoperable solutions, Privacy by Design is not common practice.
2. Consent by the data subject is often applied as legal basis in the private sector. This sometimes leads to a more relaxed attitude to data minimisation ('the client is OK anyway').
3. Mechanisms to acquire consent as implemented by service providers are often inadequate: packaged in lengthy agreements, lacking clarity and/or not providing the required information to the data subject.
4. Data protection supervisors have insufficient resources for investigations and enforcement.
5. In some cases local political decisions lead to inconsistency as to what is allowed/required with respect to personal data protection, particularly across borders.
6. Controllers outside the EU do not fall within the scope of the existing European data protection framework, although they may process personal data of EU inhabitants.

Extensive responses from the Slovenian Information Commissioner (ICRS) and ICO in the UK included some additional views of which the most important are listed below.

ICRS:

1. In our view the co-operation between the industry and EU level entities could be improved. Codes of practice and other frameworks developed together might be the most appropriate tool (for example the recently developed RFID PIA framework) so we strongly support this kind of cooperation to deal with the problem of abstractness and harmonization of the legal framework. [*In response to the question whether further specifications or codes of practice, coordinated at EU level would improve the current situation of uncertainty and occasional inconsistency between*

member states]

2. In terms of ITS as much as possible should be done at EU level in order to avoid negative consequences, such as higher costs, diverging regimes. For example, in the case of electronic toll collection an EU wide system should be developed and in doing so data protection principles should be incorporated already from the design stages. Bearing that in mind serious considerations should be given to on-board devices that are capable of performing in anonymous modes and able to support a variety of services (toll collection, PAYD insurance etc.) in a way acting as data mediators or identity providers that give only as much data away as needed for a particular service. [*In response to the question whether the different data protection regimes in Europe are regarded as a major issue for ITS development and compliance*].
3. We are of the opinion that when speaking about interests of prevention, investigation, detection, prosecution of criminal offences or national security a particular *privacy impact assessment* should be carried out. Taking into account the particularities of the field that you also describe, both ex-ante as well as ex-post evaluation of this interests should be performed in order to comprehensively assess whether the measures are: *necessary*, *proportionate* and *effective*. It also needs to be stressed that law enforcement often will not even need additional legal ground to access personal data processed through (new) ITS systems due to their existing general competencies to access data. We do not see major changes in this respect with the adoption of the proposed new EU legislation, but rather an *increased importance of the privacy by design concept* (this gives very different results in for example the case of large new centralized databases with locations of drivers where law enforcement could access large amounts of personal data in contrast with annonymous or decentralized solutions). The aspect of law enforcement should also be discussed in the proportionality tests. [*In response to a question on the issue that personal data processed by ITS are used for purposes of prosecution, criminal investigation etc., i.e. outside the scope of the data protection directive*]

The ICO's feedback included the following remarks:

1. Sector-specific data protection guidance could help but also restrict harmonisation and may result in uncertainty and complication rather than clarity. If the EU would produce guidance and a data protection authority disagrees, or their domestic legislation

stipulates to the contrary, issues would present, regardless of whether or not the guidance was binding.

2. (Specific) PIA templates are useful but should enable authorities to amend the PIA as required, recognising the myriad of circumstances in which they operate.
3. ICO is not looking for a separate framework for ITS on EU level, being conscious of fair-trading and financial regulations (for example), which might not have a clear cross-European approach.

4.1.5. STATUS OF SPECIFIC GUIDANCE ON ITS

From the analysis of specific applications in Section 3. it is concluded that ITS applications have been covered by opinions that provide specific guidance as to how personal data protection should be taken care of. These opinions are issued by national data protection supervisors, the Art. 29 WP, the IWGDPT or the EDPS. From a content perspective the opinions – in case more opinions were published on the same subject – are consistent on headlines. The following issues are noted however:

1. Some areas/applications are well-covered, others only partially and most applications are not covered at all.
2. Due to their different origins, the applicability (country, type of organisation) differs.
3. Some applications are covered by detailed guidance. This is – understandably – the case for applications that are regulated on a European level (eCall, Digital Tachograph). In other cases however, the recommendations are on headlines only and many vital questions on data protection are left open.

4.2. Relevant policy instruments of the EU

The EU disposes of different types of instruments to implement policies:

- legislative instruments (regulations, directives and decisions),
- non-binding instruments (recommendations and opinions)
- financial instruments (e.g. funding for research or standardisation)
- enforcement instruments (sanctions and legal action) in case primary or secondary legislation is in place that mandates such enforcement.

In general, legal instruments have a strong impact once fully adopted, yet may take many years to prepare and implement. Non-binding instruments can be implemented much faster, yet will only be effective if sufficiently supported by the Member States and other main stakeholders.

As extensively discussed in this document, see 2.1.2, a new legal framework for personal data protection in the EU has been prepared and is currently discussed

with the Member States. It is likely that the new framework will be adopted, probably after various modifications. It is noted that the regulation proposal, [18] Art. 86, provides the Commission with powers to adopt delegated acts for a further specification of conditions for and requirements on personal data processing in various sectors and data processing situations. In principle – and under certain conditions – the EC would be given the powers to define detailed requirements on personal data processing requirements in specific ITS areas and applications.

4.3. Analogy of smart metering in the energy sector

In the last decade a development has started that will lead to a drastic modernisation of the electric grid. The so-called Smart Grid will bring higher efficiency and flexibility for distributed generation and storage of electricity. It is expected to enable a better balance between time-based supply and demand, and to create consumer awareness on energy-efficient behaviour. The Smart Grid is an important component of a sustainable energy policy. As the energy sector is by nature strongly regulated, and benefits of European harmonisation in this area are generally recognised, several initiatives were taken at a European level to produce a set of regulatory recommendations to ensure EU-wide consistent, cost-effective and fair implementation of Smart Grids. One of these initiatives was the foundation of the Smart Grids Task Force. The Smart Grids Task Force includes a dedicated Expert Group (EG2) on privacy, security and data safety, which produced its regulatory recommendations in 2011, see [76]. The Expert Group 2 is currently elaborating a Privacy Impact Assessment template, which is to be issued in the 4th quarter of 2012.

Smart metering is a key component of the Smart Grid. The smart meter measures and stores information on electricity consumption (and supply) in the end nodes of the grid and has data communication capability which enables the remote use of time-slotted consumption data. Such data are useful for more efficient network load management, more fine-grained tariff policies for demand management and to provide users with better information on their usage, stimulating energy savings. The challenge of smart metering is that electricity consumption data on the level of individual households is to be considered as personal data. Depending on the level of detail, it may e.g. reveal when people leave home and when they return, when they are on holidays and when certain appliances with a relatively high consumption are switched on and off. The potential impact of smart metering on personal data protection was recognised from the start and this allows for a fundamental approach to data protection, a true privacy by design approach, see [75] for an overview. Recommendations for further regulatory frameworks include:

- Build in privacy features in the governance framework, apply privacy into the design. PIA's should be conducted in requirements analysis and

design stages. One of the key points is that for most purposes, detailed household data are not required, and central processing of such can be avoided. Techniques have been developed that allow load monitoring on an (arbitrary) higher level of aggregation, but do not disclose meter readings on household level.

- Privacy by Default. Where options leading to disclosure of (more) personal data are provided, based on positive consent, the standard or 'no user action taken' situation should always imply the maximum protection / minimum disclosure of data.
- Data minimisation, and local (in the smart meter) secure processing of data where possible. This would provide the user with all meaningful detailed information but only send aggregated data for billing to the backoffice. This is quite similar to concepts for road pricing and pay as you drive insurance as discussed in Sections 3.2.3 and 3.2.6.
- Avoid trade-offs between privacy and other legitimate objectives. It is believed that a true PbD approach allows respecting of all interests.
- Maintain privacy and data security end-to-end. This refers to using encryption, pseudonymisation and measures against traffic analysis when personal data are exchanged over public networks, maintaining a minimum number of storage locations for data, maintaining need-to-know access to personal data and secure erasure of data when no longer required for the purpose.
- Visibility and transparency to the consumer.

The recommendations above are quite similar to PbD approaches and practices that are applied or at least have been recommended for a number of ITS applications. The main lesson to learn from the smart grid development is that it proved possible to bring together the various stakeholders in the sector and to build consensus on how to come to privacy-friendly solutions while respecting the main objectives. This as opposed to a situation where data protection supervisors develop sector or application-specific guidance without involvement of the industry and the industry develops standards and solutions without (full) consideration of this guidance.

It is noted that the Smart Grid is a development of great importance and impact where the benefit of EU coordination and guidance is generally acknowledged. This may not be the case for applications that have a local scope and where significantly different approaches coexist between countries, and applications in the private domain.

It can be argued however that concerning ITS, cooperative systems and services constitute a paradigm change comparable to the Smart Grid in the energy sector. Cooperative systems and services will drastically change the amounts and places of processing of mobility data. In addition, for a successful implementation, high

requirements on interoperability, reliability and safety across borders have to be satisfied. This suggests that, as with the Smart Grid, data protection supervisors and industry should join forces to build privacy into the DNA of the technology in basic standards and from the early stages of development of cooperative systems and services.

4.4. Contribution from PRESERVE project

A specific contribution to this study was provided by the European R&D project PRESERVE, [77].The document identifies a number of barriers for the adoption of PbD and suggests measures to address these barriers. In fact, most of the issues and solutions are not specific for ITS.

The most relevant and straightforward recommendations are summarised below:

- Policy makers must ensure that appropriate technology support (for personal data protection) is made available. This can lead to requirements for integrating security support in communication systems.
- As to practicing Privacy-by-Design it is recommended to create awareness as well as experience on minimization, enforcement and transparency measures.
    - In particular, focused academic research is taking place on minimization techniques. However such expertise is not common in the industry.
    - Little research work is available on enforcement for privacy. But this work could leverage on well-established work on enforcement of access restrictions.
    - Little research work is available on transparency support.
- It is recommended to start re-assessing existing development processes and assess how they should be amended to support PbD
- It is recommended to add courses related to privacy and Privacy-by-Design in the ICT and engineering education curricula.
- It is recommended that more research is done to find more flexible approaches to support the dynamic deployment of measures for minimization, enforcement and transparency. This should apply even during operations of large-scale systems, to cope with the ineluctable evolution of threat models and technology.

4.5. iMobility Forum

The iMobility Forum is a joint platform for all parties interested in ICT-based systems and services in the mobility sector. Its field of work includes ICT systems for resource-efficient and clean mobility in addition to ICT-based safety

technologies. The iMobility Forum succeeds the eSafety Forum and has members from the entire ITS value chain. The steering committee is chaired by the EC.

Currently the iMobility Forum Legal WG is working on a report that will include recommendations on privacy issues in the area of ITS. The document was not yet available at the date of issue of this report.

4.6. Discussion and selection of possible measures

In Section 4.1, some perceived privacy concerns of different types stakeholders were listed. It can be observed that the concerns are often not specific to ITS and partly overlapping between types of stakeholders.

The good thing is that measures can be defined that target various concerns at the same time. As an example, a lack of clarity or guidance felt by the industry on one hand, and a lack of adoption of privacy by design observed by data protection supervisors on the other hand, may be solved by a serious effort of the industry to elaborate sector-specific solutions. The following measures are deemed appropriate:

- Guidance for design and operations regarding personal data protection in ITS should be provided. An ITS PIA template - see [85] as an example of such a document elaborated for RFID applications - is expected to be an effective and appropriate instrument. Further application specific guidance may take the form of design principles and criteria, design methods, PETs, security measures, codes of practice and PIA frameworks or templates tailored for a specific application (area). The EC should coordinate this process to make sure results are delivered and to stimulate broad adoption throughout the EU. The development requires strong support from the ITS industry, and may involve public sector stakeholders where appropriate. Data protection supervisors should preferably provide advice, review results and finally be part of a consensus process.
- In terms of application-specific guidance, the first candidate applications would be those that have the greatest potential impact on privacy, in particular those that process more detailed and more complete mobility patterns and potentially affect large groups of users. The following applications and themes should have priority:
  - Cooperative Systems, see also below.
  - Road User Charging on extended networks, involving passenger cars
  - E-ticketing in public transport

- Pay-as-you-drive insurance
- Floating Vehicle Data
- Policies and mechanisms for consent for services delivered or enabled by in-vehicle platforms, addressing issues of different drivers/passengers using a car and different but bundled applications sharing an in-car platform.
- Rules, methods and criteria how geolocation data can be kept for non-personalised purposes (e.g. traffic forecasts, urban planning, vehicle performance analysis).

- In case it proves infeasible to trigger the industry to strongly participate in developing guidance in specific areas of ITS, the EC may ask the Art. 29 WP to prioritise certain ITS themes. This is regarded as a second-best option as it does not tackle the issue felt by the industry that data protection supervisors sometimes have insufficient understanding of the practical challenges of ICT and operations to define optimum solutions.
- Cooperative systems form a special category of concern as it is an application area with a potential to completely change road transport as we know it today and would – on a longer term – affect all vehicles and all vehicle trips. Given the challenges it involves concerning privacy, it requires coordination and further elaboration on a European level involving at least the automotive industry and road operators.
- Require, wherever possible, that personal data protection expertise is involved in the development of ITS standards and (EU funded) R&D efforts. In the current situation, standards development within CEN, ISO and ETSI is driven by the industry and predominantly involves technical experts. There are insufficient guarantees that the interest of personal data protection and the required expertise is always sufficiently represented in the work groups and project teams that prepare standards which should constitute the building blocks for privacy by design. This also applies to the ITS R&D community.

4.7. Recommendations

Recommendation 1.
The EC should take the initiative to prepare concrete guidance on personal data protection for specific applications and aspects of ITS. Such guidance should take the form of a Privacy Impact Assessment template for ITS applications and services. Apart from clearly describing a PIA method and procedure, it should preferably include guidance for Privacy by Design methods and criteria, PETs, security measures and codes of practice. Such generic PIA template should be complemented with tailored guidance for applications or application areas of particular concern from a personal data protection perspective. The industry and consumer organisations should be invited to participate in the development of the PIA template. The Art. 29 Working Party should be invited to provide advice, review results and finally endorse the outcome.

Recommendation 1A.
Cooperative applications would deserve a dedicated approach because of the vast amounts of geolocation data that will be processed (in the future possibly concerning all car users), the resulting potential impact on privacy, as well as the opportunity to influence such developments before their large-scale deployment.

Recommendation 1B.
Specific attention should further be paid to:

- Road User Charging on extended networks, involving passenger cars
- E-ticketing in Public transport
- Pay-as-you-drive Insurance
- Floating Vehicle Data
- Policies and mechanisms for user consent for services delivered or enabled by in-vehicle platforms, addressing issues of different drivers/passengers using a car and various applications sharing one in-car platform
- Rules, methods, tools and criteria for storage of geolocation data / mobility patterns for non-personalised purposes (e.g. traffic forecasts, urban planning, vehicle performance analysis).
- The impact of complex data protection responsibilities in ITS service chains that have multiple or joint processors and controllers.

Recommendation 2.
The EC should assert that data protection expertise is involved in standardisation working groups and the ITS R&D community as these establish the fundament and building blocks on which Privacy by Design or Privacy Enhancing Architectures are to be realised. The EC should discuss this with standardisation bodies and the ITS R&D community and should include it as a requirement when issuing mandates to CEN and ETSI for developing standards in specific ITS areas.

5. Conclusions

Generic findings

17 years after the adoption of the data protection directive it may be concluded that its concepts and principles have proven to be a stable and useful legal basis for personal data protection in the EU. The national legal implementations and practice of data protection have nevertheless led to a fragmentation of the implementation of personal data protection across the European Union. It is also observed that strong developments in the area of computing, internet, mobile communications, social media and the massive use by consumers pose new challenges for personal data protection. The existing framework is not fully adequate/effective to cope with these challenges.

The EC is currently preparing a new legal framework for personal data protection in the EU. Its aim is not to change the objectives and principles, but to improve the inconsistencies and inefficiencies of the current constellation. With respect to harmonisation, refinements to the definition and rules for 'unambiguous user consent', 'the right to be forgotten' and liability of the processor, these are expected to improve legal certainty for both controllers and data subjects. Enforcement is expected to become more effective as sanctions will have to be specified for different categories of data protection regulation violations. Efficiency is expected to be gained by reducing the administrative burden for processing situations that have limited privacy risks whilst at the same time imposing higher administrative requirements on high-risk processing situations. The rules for transfer of personal data to third countries are simplified as prior authorisation is not required anymore where a transfer is based on standard data protection clauses or binding corporate rules. These modifications are of course not specific for ITS, but the areas of improvement certainly apply to many services in that area.

Sector-specific guidelines

Both in the existing and proposed new legal framework, a fundamental question is what additional sector or application specific rules and methods (whether mandatory or self-imposed) are useful to improve data protection in ITS applications. Whereas specific guidelines might increase clarity and consistency within an application area, significant differences in objectives, users groups, size and scope between deployments render it challenging to formulate specific solutions or constraints that would apply to all situations. Formulating guidelines on a somewhat higher level of abstraction can be useful but has the risk of adding little value to the legislation itself.

When schemes are introduced that affect large groups of private users and that have a mandatory element, e.g. in the area of passenger car road pricing or e-ticketing, arrangements for personal data protection are often subject to public

debate and of political importance. As a consequence, the outcomes in one country are not fully predictable and not necessarily consistent with outcomes in another country. The trade-off between important interests such as efficiency, enforcement/fraud prevention, flexibility, ease of use and user privacy is never absolute and in such cases made in the political domain.

Analysis of applications

The assessment of 10 different ITS applications allows for some interesting observations:

- Some areas have had abundant coverage by specific opinions concerning data protection issues involved. Other areas much less. This is not always in relation to the risks involved.
- In the perception of the user, as well as in the legal basis, there is a clear distinction between services (or elements of it) an individual chooses or agrees to out of free will and things he is forced to accept because there is simply no alternative if he for example wishes to use his car, park it on-street or use the public transport. It is observed that often services start with a voluntary character but gradually develop into situation where no alternative, or only an alternative that is inferior or limited in options is available. As an example, consider a situation where e-ticketing is first marketed as a voluntary option of convenience for frequent users but gradually develops into a scheme where paper tickets are no longer accepted. There is a risk that data protection measures developed for the situation based on voluntary use are not, or cannot be transformed to, an adequate arrangement for mandatory use.
- Personal data processing in ITS systems often concern location data, i.e. collections of locations and associated time stamps that can (with a varying level of difficulty) be traced to an individual. Some applications only process occasional samples of location data, e.g. parking payment or local section speed control systems. Other applications by their nature collect vast amounts of location data that might in an extreme case constitute complete mobility patterns of a person or vehicle (to which a natural person can often be linked with a high probability). This can notably the case for GNSS-based road user charging, e-ticketing in public transport, pay-as-you-drive insurance, fleet monitoring and floating cellular/vehicle data for traffic information. Such applications deserve special attention from a data protection point of view, as the potential privacy infringement resulting from unauthorised access to or misuse of such data is considerable.

  It seems worth noting that threats involving processing personal mobility data are not the exclusive domain of ITS: the spectacular development in

the uses of GNSS- and WiFi capable mobile phones create at least comparable issues. This area has been subject to dedicated opinions including one of the Art. 29 Working Party. Part of these recommendations could apply to ITS applications as well.

- In applications where extensive/detailed location data needs to be processed, some approaches that provide a significant improvement as to personal data protection can often be applied:
  - *Pseudonymisation*: by using short-lived identifiers the possibility of identification of individual users from the data processed can be eliminated or strongly reduced. This is particularly relevant in the context of cooperative systems.
  - *Distributed processing*: when an identification cannot be avoided, e.g. because there is a central billing process, the detailed location data may be needed to calculate the information required, but only the aggregated results are required for the central processing. In this case, a so-called smart or thick client architecture may be applied. The On-Board Equipment or user device processes location details, but only the aggregated results are uploaded to the central system. A further improvement is realised when *Data Subject Control* is implemented: the user can inspect and delete the stored details. It is noted that a thick client approach has advantages in terms of data protection as well as communication requirements, but introduces complexity in the area of security, compliance checking, application management and appeal processes. This measure is particularly applicable in the area of PAYD insurance, GNSS-based Road Pricing systems and Floating Vehicle Data. In essence, a thick-client approach also applies to eCall and the Digital Tachograph.
  - *Domain separation*. The location details / usage details are labelled with identifiers that do not allow straightforward identification and are strictly shielded from the billing domain where contract ID's and person details are used. This measure is generally not as powerful as a thick client approach and does not eliminate the possibility of identification but still reduces risks.
  - *Deletion/anonymisation immediately after initial processing*. Data allowing identification may immediately after (almost) real time processing, and in the equipment where the data are collected (camera or receiver), be deleted or any unique identifier may be removed. This is applicable in travel time measurements by roadside observation and in section speed control systems.
  - *Data minimisation*. This is more a general requirement following from the data protection directive than a specific measure. Nevertheless it deserves mentioning that it is often possible to

reduce the information that is processed based on the service options that are actually selected as compared to an approach where a superset of data is collected by default.

Privacy by Design

Developments in several areas of ITS imply ever increasing challenges to the privacy of travelling individuals. A thorough Privacy Impact Analysis (PIA) combined with a real implementation of Privacy-by-Design throughout the development process can be expected to reduce the risks to a minimum. The PIA should lead to a balanced and somehow quantified and objective outcome in terms of privacy risks. Identified high risks should lead to 'must have' requirements on the solution. The design process should start with determining an optimum solution/architecture (multiple criteria) and set of PETs (Privacy Enhancing Technologies), that at least satisfy these requirements. For ITS applications the set of design principles/PETs listed in the previous paragraph are particularly relevant. The Privacy-by-Design process should assert that the privacy-driven requirements are elaborated and taken along in the entire development process, from global design to validation and verification. At this point, it is not clear if, how and when Privacy-by-Design will be transformed from a vision of legislators into something applied in the engineering department.

Recommendations

The type of problems that stakeholders are faced with regarding data protection / privacy depend on their perspective. Industry and data protection supervisors are regularly at opposite sides of the table. Individual data subjects often have yet another angle. It is felt however that all stakeholders will benefit if:

- personal data protection is adequately addressed in the fundament of services and applications
- clear methods, rules and approaches to comply with data protection legislation are available
- new services that add efficiency, safety or comfort are not hampered by unnecessary restrictions
- data subjects feel well-informed and comfortable concerning their privacy when using new services and applications.

To realise this vision in the area of ITS however, it seems that more coordination and more cooperation between stakeholders is needed. This leads to the following recommendations:

Recommendation 1.
The EC should take the initiative to prepare concrete guidance on personal data protection for specific applications and aspects of ITS. Such guidance should take the form of a Privacy Impact Assessment template for ITS applications and services. Apart from clearly describing a PIA method and procedure, it should preferably include guidance for Privacy by Design methods and criteria, PETs, security measures and codes of practice. Such generic PIA template should be complemented with tailored guidance for applications or application areas of particular concern from a personal data protection perspective. The industry and consumer organisations should be invited to participate in the development of the PIA template. The Art. 29 Working Party should be invited to provide advice, review results and finally endorse the outcome.

Recommendation 1A.
Cooperative applications would deserve a dedicated approach because of the vast amounts of geolocation data that will be processed (in the future possibly concerning all car users), the resulting potential impact on privacy, as well as the opportunity to influence such developments before their large-scale deployment.

Recommendation 1B.
Specific attention should further be paid to:

- Road User Charging on extended networks, involving passenger cars
- E-ticketing in Public transport
- Pay-as-you-drive Insurance
- Floating Vehicle Data
- Policies and mechanisms for user consent for services delivered or enabled by in-vehicle platforms, addressing issues of different drivers/passengers using a car and various applications sharing one in-car platform
- Rules, methods, tools and criteria for storage of geolocation data / mobility patterns for non-personalised purposes (e.g. traffic forecasts, urban planning, vehicle performance analysis).
- The impact of complex data protection responsibilities in ITS service chains that have multiple or joint processors and controllers.

Recommendation 2.
The EC should assert that data protection expertise is involved in standardisation working groups and the ITS R&D community as these establish the fundament and building blocks on which Privacy by Design or Privacy Enhancing Architectures are to be realised. The EC should discuss this with standardisation bodies and the ITS R&D community and should include it as a requirement when issuing mandates to CEN and ETSI for developing standards in specific ITS areas.

6. Bibliography

[1] Task specifications to award a specific contract to assess the security and personal data protection aspects related to the handling of data in ITS applications and services and propose measures in full compliance with Community legislation ; EC DG MOVE Unit C3 ; September 2011.D1 Inception Report task 5.1 ; 20120221ITSAP5 1_D1v1.4 ; Algoe/Rapp Trans ; March 6th 2012.

[2] Action Plan for the Deployment of ITS in Europe; COM2008 886; European Commission; 2008. Directive 2010/40/EC laying down the framework for the deployment of ITS in the field of road transport and for interfaces with other modes; European Union; 2010.

[3] Inception report – Action 5.1 ITS Action Plan; Algoé & Rapp Trans; Version 1.3; February 2011.

[4] Directive 95/46/EC on on the protection of individuals with regard to the processing of personal data and on the free movement of such data; European Union; 1995.

[5] Opinion of the European Data Protection Supervisor on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe and the accompanying proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes; 2010/C 47/02; European Data Protection Supervisor; July 2009.

[6] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ; the Organization for Economic Co-Operation and Development ; January 1999 (updated) ; http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

[7] The Right to Privacy ; Warren and Brandeis ; Harvard Law Review, Vol. IV, December 15, 1890, No. 5.

[8] EC Study on implementation of the data protection directive - Comparative summary of national laws ; Douwe Korf, Human Rights Centre, University of Essex, UK ; September 2002 ; http://www.garanteprivacy.it/garante/document?ID=455584.

[9] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ; July 2002 ; amended in 2009.

[10] European Convention on Human Rights and Fundamental Freedoms ; Council of Europe ; November 1950.

[11] PSC Recommendations to the ISO/TMB, ISO/TMB/PSC N0123, 10 January 2012.

[12] ISO/IEC 29100:2009 Information Technology – Security Techniques – Privacy Framework ; ISO IEC JTC1/SC27; 2009.

[13] CWA 16113:2010, CEN Workshop Agreement - Personal Data Protection Good Practices; June 2010.

[14] ISO/TR 12859:2009 Intelligent Transport Systems – System Architecture - Privacy aspects in ITS standards and systems; 2009.

[15] ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements.
[16] ISO/IEC 27002:2005 Information technology -- Security techniques – Code of practice for information security management.
[17] A comprehensive approach on data protection in the EU; COM(2010)609; EC Communication; November 2010.
[18] Proposal for a regulation of the EP and of the Council on the protection of personal data with regard to the processing of personal data and on the free movement of such data (general data protection regulation); COM(2012)11; EC Communication; February 2012.
[19] Proposal for a directive on the protection of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the free movement of such data ; COM(2012)10; EC Communication; January 2012.
[20] Projet de règlement européen: la défense de la vie privée s'éloigne du citoyen (Proposal for a Regulation: protection of privacy is moving away from the citizen) ; CNIL publication ; January 2012 ; http://www.cnil.fr/dossiers/vie-citoyenne/actualites/article/projet-de-reglement-europeen-la-defense-de-la-vie-privee-seloigne-du-citoyen-1/.
[21] Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters ; Council of the EU; November 2008.
[22] Note regarding the Proposal for a directive on the protection of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the free movement of such data ; Presidency of the Council of the EU ; 8596/12 ; April 2012.
[23] Summary of replies to the public consultation about the future legal framework for protecting personal data ; European Commission DG JUST ; November 2010.
[24] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC ; European Union ; March 2006.
[25] Working party 29 - Opinion 13/2011 on Geolocation services on smart mobile devices on the use of location data with a view to providing value added services; WP185; May 2011.
[26] Working party 29 - Opinion on the use of location data with a view to providing value added services; 2130/05/EN - WP115; November 2005.
[27] Common position on privacy of location information in mobile communications services ; International Working Group on Data Protection in Telecommunications ; 675.29.8 ; November 2004.
[28] Opinion of the European Data Protection Supervisor on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe and the accompanying proposal for a Directive of the European Parliament

and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes; EDPS; 2010/C 47/02; February 2010.

[29] Vulnerabilities in Electronics and Communications in road transport: Discussion and Recommendations; eSecurity Working Group / eSafety Forum; June 2010.

[30] Opinion of the Slovenian Information Commissioner on the protection of personal data in the electronic road toll system ; IP-RS ; 2008.

[31] Het advies van 30 september 2008 inzake het wetsvoorstel kilometerprijs (Advice on NL road pricing plans) ; College Bescherming Persoonsgegevens (NL) ; Sept 2008 ; http://www.cbpweb.nl/downloads_adv/z2008-01050_2.pdf

[32] Report and Guidance on Road Pricing- ”Sofia Memorandum” ; IWGDPT 45th meeting, 12-13 March 2009 Sofia (Bulgaria) ; March 2009 ; http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

[33] Study on the economic benefits of privacy•]enhancing technologies (PETs) ; Final Report to the EC, DG JUST ; London Economics ; July 2010.

[34] White Paper for Decision Makers ; Koorn, R., Borking, J., van Gils, H., ter Hart, J., Overbeek, P. and Tellegen, R. Ministry of the Interior and Kingdom Relations (NL), 2004.

[35] Council Regulation (EEC) of 20 December 1985 on recording equipment in road transport, (various amendments) ; No 3821/85 ; December 1985 (last amended October 2011).

[36] Opinion of the EDPS on Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EEC) No 3821/85 on recording equipment in road transport and amending Regulation (EC) No 561/2006 of the European Parliament and the Council Official Journal C 037 , 10/02/2012 P. 0006 – 0013, October 2011.

[37] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Council Regulation (EEC) No 3821/85 on recording equipment in roadtransport and amending Regulation (EC) No 561/2006 of the European Parliament and the Council ; COM(2011) 451 final ; July 2011.

[38] Guidlines for personal data protection in employment relationships ; Information Commissionner RS ; April 2008; https://www.iprs.si/fileadmin/user_upload/Pdf/smernice/Guidelines_Employment.pdf

[39] Rapport van bevindingen - Ambtshalve onderzoek CBP naar de verwerking van geolocatiegegevens door TomTom N.V. ; College Bescherming Persoonsgegevens (NL) ; December 2011.

[40] Preserving Privacy in GPS Traces via Uncertainty-Aware Path Cloaking; Proceedings of the 14th ACM conference on Computer and communications security; Baik Hoh, Marco Gruteser, Hui Xiong and Ansaf Alrabady; Rutgers University NJ USA ; 2007.

[41] Mix zones: User privacy inlocation-aware services ; A. Beresford and F. Stajano ; IEEE PerSec ; 2004.

[42] ISO 24100:2010 - Intelligent transport systems -- Basic principles for personal data protection in probe vehicle information services ; 2010.
[43] PRECIOSA D1 – V2X Privacy Issue Analysis ; EC FP7 Programme ; November 2009.
[44] Pay-as-you-Drive Vehicle Insurance as a Tool to Reduce Crash Risk: Results so far and further potential ; Jan Willem Bolderdijk and Linda Steg ; University of Groningen (NL) ; Discussion paper 2011-23 ; OECD International Transport Forum ; September 2011.
[45] Délibération 2010-096 du 8 avril 2010 portant recommandation relative à la mise en œuvre, par les compagnies d'assurance et les constructeurs automobiles, de dispositifs de géolocalisation embarqués dans les véhicules ; CNIL (F) ; April 2010.
[46] Erläuterungen zu Pay as you drive (PAYD) und dem Einsatz von Black Boxes in Motorfahrzeugen ; EDOB (CH) ; May 2008.
[47] Section Control: towards a more efficient and better accepted enforcement of speed limits? – Speed Fact Sheet ; ETSC ; September 2009.
[48] OM-Cassatie, Vialis- en ANPR gegevens ; LJN : BR0554, Hoge Raad,10/05492 ; 20 September 2011.
[49] Working paper – E-Ticketing in Public Transport; IWGDPT; 675.35.12; September 2007.
[50] Study on data collection and storage in the EU ; European Network and Information Security Agency ; February 2012.
[51] Study on electronic ticketing in public transport – Final Report; Mohamed Mezghani – EMTA ; May 2008.
[52] Délibération n°AU-015, 28-4-2011 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel relatifs à la gestion des applications billettiques par les exploitants et les autorités organisatrices de transport publics ; CNIL (F) ; April 2011.
[53] Intelligent Transport Systems (ITS) – Security – Threat, Vulnerability and Risk Analysis (TVRA) ; ETSI TR 102893 V1.1.1 ; March 2010.
[54] PRECIOSA D11 – Guidelines for Privacy Aware Applications ; EC FP7 Programme ; March 2011.
[55] EDPS comments on the Commission Recommendation and the accompanying impact assessment on the implementation of the harmonised EU-wide in-vehicle emergency call; EDPS; December 2011.
[56] WP29 - Opinion on data protection and privacy implications in eCall initiative - 1609/06/EN - WP125 ; WP29 ; September 2006.
[57] EN 15722 Intelligent transport systems — eSafety — eCall minimum set of data (MSD) ; Edition: 2011-11-01.
[58] Report and Guidance on Road Pricing - "Sofia Memorandum" ; 675.38.12 ; IWGDPT ; March 2009.
[59] Opinion of the Slovenian Information Commissionner on personal data protection in the electronic toll system ; IC-RS (SI); July 2008.

[60] Het advies van 30 september 2008 inzake het wetsvoorstel kilometerprijs (Advice on NL road pricing plans) ; z2008-01050 ; CBP (NL) ; http://www.cbpweb.nl/downloads_adv/z2008-01050_2.pdf
[61] Regels voor het in rekening brengen van een gebruiksafhakelijke prijs voor het rijden met een motorvoertuig (Wet kilometerprijs) [Road Pricing Act, NL] ; 200910898 ; November 2009 ; http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2009/11/13/200910898-aanbieding-documenten-wet-kilometerprijs.html
[62] ISO/TS 12813:2009 Electronic fee collection -- Compliance check communication for autonomous systems ; ISO Technical Standard ; November 2009.
[63] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport ; EU ; July 2010.
[64] PRESERVE Deliverable 1.1 - Security Requirements of Vehicle Security Architecture ; version 1.00 ; IST-269994 ; June 2011.
[65] Secure Vehicle Communication Deliverable 2.1 - Security Architecture and Mechanisms for V2V/V2I ; February 2008.
[66] PRECIOSA D7 Privacy Verifiable Architecture ; EC FP7 project ; July 2009.
[67] Opinion 15/2011 on the definition of consent ; Art. 29 Data Protection Working Party ; 01197/11/EN WP187 ; July 2011.
[68] Wi-Fi Positioning Systems: Beware of Unintended Consequences - Issues Involving the Unforeseen Uses of Pre-existing Architecture ; Information and Privacy Commissioner Ontario, Canada ; June 2011.
[69] Délibération n°2009-002 du 20 janvier 2009 de la formation restreinte prononçant un avertissement à l'encontre de la société KEOLIS RENNES; CNIL, France; January 2009.
[70] LJN: BR0554, Uitspraak Hoge Raad der Nederlanden, 10/05492, Strafkamer; Rechtspraak, Nederland; September 2011.
[71] Délibération n°2011-035 du 17 mars 2011 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société GOOGLE Inc.; CNIL, France; March 2011.
[72] Joined Cases C-465/00, C-138/01 and C-139/01 (Judgment of 20 May 2003) / Reference for a preliminary ruling from the Verfassungsgerichtshof and Oberster Gerichtshof: Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and between Christa Neukomm (C-138/01), Joseph Lauermann (C-139/01) and Österreichischer Rundfunk (Protection of individuals with regard to the processing of personal data — Directive 95/46/EC — Protection of private life — Disclosure of data on the income of employees of bodies subject to control by the Rechnungshof); European Court of Justice; May 2003.
[73] C-553/07 College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer Netherlands (judgement of 7 May 2009) / Protection of individuals with regard to the processing of personal data - Directive 95/46/EC - Respect for private life - Erasure of

data - Right of access to data and to information on the recipients of data - Time-limit on the exercise of the right to access; European Court of Justice; May 2009.
[74] C-468/10 and C-469/10 Judgment of the Court (Third Chamber) of 24 November 2011 (references for a preliminary ruling from the Tribunal Supremo — Spain) — Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10), Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v Administración del Estado Processing of personal data — Directive 95/46/EC — Article 7(f) — Direct effect; European Court of Justice; November 2011.
[75] Smart Meters in Europe, Privacy by Design at its Best; Information and Privacy Commissioner Ontario, Canada; April 2012.
[76] Regulatory Recommendations for Data Safety, Data Handling and Data Protection; Task Force Smart Grids, Expert Group 2; February 2011.
[77] PRESERVE Contribution to ITS Data Protection Study; Antonio Kung; July 2012.
[78] Treaty on the functioning of the European Union (TFEU); May 2008.
[79] Charter of fundamental rights of the European Union; 2000/C 364/01; December 2000.
[80] Working paper – Event Data Recorders on Vehicles – Privacy and data protection issues for governments and manufacturers; Ref. 675.42.10; International Working Group on Data Protection in Telecommunications; April 2011.
[81] The digitization of the public domain; Rathenau Institute; Christian van 't Hof and Wouter Schipzand; October 2008; http://www.rathenau.nl/en/publications/publication/near-field-communication-1.html.
[82] PriPAYD: Privacy Friendly Pay-as-you-drive Insurance; C. Troncoso, G. Danezis, E. Kosta, and B. Preneel, Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society; 2007.
[83] Consensus paper on privacy in transport IFM applications, Deliverable 2.2, Version 4.3, IST-2007-214787, Interoperable Fare Management Project; EU 7th Framework Project; December 2009.
[84] Legal framework and requirements of automotive on-board networks, Deliverable D2.4, EVITA, EU 7th Framework Project; September 2011.
[85] Privacy and Data Protection Impact Assessment Framework for RFID Applications; European Commission, DG CONNECT; January 2011; http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf.
[86] 120620ITSAP 5 1_D3 Workshop Report v2.0.doc; Rapp Trans; June 2012.