PD CEN/TR 16742:2014

BSI Standards Publication

Intelligent transport systems — Privacy aspects in ITS standards and systems in Europe

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CEN/TR 16742:2014. It supersedes PD ISO/TR 12859:2009 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee EPL/278, Intelligent transport systems.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 79082 9

ICS 35.240.60

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 October 2014.

Amendments issued since publication

Date	Text affected

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 16742

October 2014

ICS 35.240.60

English Version

Intelligent transport systems - Privacy aspects in ITS standards and systems in Europe

Systèmes de transport intelligents - Aspects de la vie privée dans les normes et les systèmes en Europe

Intelligente Transportsysteme - Datenschutz Aspekte in ITS Normen und Systemen in Europa

This Technical Report was approved by CEN on 23 September 2014. It has been drawn up by the Technical Committee CEN/TC 278.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. CEN/TR 16742:2014 E

Contents

Page

Foreword

This document (CEN/TR 16742:2014) has been prepared by Technical Committee CEN/TC 278 “Intelligent transport systems”, the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

Introduction

This Technical Report is a guide for the developers of both ITS itself and its standards when many types of data are exchanged during the performance of its tasks, which includes in some cases personal data and information. Such Personal Data or Personal Information (PI) underlies for their applications special rules defined in European Union (EU) mandatory directives or a possible EU Regulation concerning the revision of the EU Directives at Data Protection or at the national level national data protection law. In order to avoid an incorrect use of PI in any standard or Technical Report, which would cause the application of this standard or Technical Specification to be banned by legal courts, this Technical Report gives guidelines for the CEN/TC 278 Working Groups how to deal with PI in compliance with the legal rules.

Even though specific data privacy protection legislation is generally achieved through national legislation and this varies from country to country there exists a basic set of rules which are common in all European countries. These common rules are defined in the European Directives 95/46/EC and 2002/58/EC in their current versions. Countries not members of the European Union (Switzerland, Norway, Island etc.) have issued national data protection laws, which are very closely aligned to the European Directives. It should also be noted that the European Directives on the protection of individuals (95/46/EC and 2002/58/EC) are regarded as the strongest legal rules around the world.

This Technical Report builds on the content of ISO/TR 12859:2009 but extends the rules and recommendations in order to be as compliant as is reasonable with the European Directives and some of the national data protection laws. This means it is more specific and includes some recent developments and it tries to include some intentions of what the European Commission is preparing to include in a revised and enforced version of the Directive 95/46/EC (the proposed EU proposal of a Regulation of data protection COM(2012)11 final, 2012/0011 (COD)).

1 Scope

This Technical Report gives general guidelines to developers of intelligent transport systems (ITS) and its standards on data privacy aspects and associated legislative requirements. It is based on the EU-Directives valid at the end of 2013. It is expected that planned future enhancements of the Directives and the proposed "General Data Protection Regulation" including the Report of the EU-Parliament of 2013-11-22 (P7_A(2013)0402) will not change the guide significantly.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
accountability
principle that individuals, organizations or the community are liable and responsible for their actions and may be required to explain them to the data subject and others and their actions shall comply with measures and making compliance evident, and the associated required disclosures

[SOURCE: ISO/IEC 24775:2011 Edition:2]

2.2
anonymity
characteristic of information, which prevents the possibility to determine directly or indirectly the identity of the data subject

[SOURCE: ISO/IEC 29100:2011]

2.3
anonymisation
process by which personal information (PI) is irreversibly altered in such a way that an Individual or a legal entity can no longer be identified directly or indirectly either by the controller alone or in collaboration with any other party

[SOURCE: ISO/IEC 29100:2011]

2.4
anonymised PI
PI that has been subject to a process of anonymisation and that by any means can no longer be used to identify an Individual or legal entity

[SOURCE: ISO/IEC 29100:2011]

2.5
committing of PI
transfer of PI from the controller to a processor in the context of a commissioned work

2.6
consent
individual's or legal entity's (data subject) explicitly or implicitly freely given agreement to the processing of its PI in the course of which the data subject has been in advance completely informed about the purpose, the legal basis and the third parties, receiving data subject's PI, and all these in a comprehensible form

2.7
controller
any natural or legal person, public authority, agency or any other body which alone or jointly with others collect and/or process and determine the purposes and means of the processing of PI, independently whether or not a person uses the PI by themselves or assigns the tasks to a processor; 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

[SOURCE: EU-Dir 95/46/EU Art 2 lit d]

2.8
data subject
any natural or legal person or association of persons whose PI is processed and is not identical to the controller or processor or third party

Note 1 to entry: ISO/IEC 29100 uses this definition for the person of which personal data are used the Principal. The above definition is that one that is used in EU-Directives.

2.9
identifiability
conditions which result in a data subject being identified, directly or indirectly, on the basis of a given set of PI

2.10
identify
establishes the link between a data subject and its PI or a set of PI

2.11
identity
set of attributes which makes it possible to identify, contact or locate the data subject

[SOURCE: ISO/IEC 29100:2011]

2.12
personal information PI
any data or information related to an individual or legal entity or an association of person or individuals by which the individual or legal entity or association of persons could be identified

Note 1 to entry: The EU-Dir 95/48/EC names in its Art 2 lit. (a) the personal information as "*personal data*" and defines it as: "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"*.

2.13
processor
natural person or legal entity or organization that processes PI on behalf of and in accordance with the instructions of a PI controller and if it use PI only for the commissioned work

2.14
sub-processor
privacy stakeholder that processes PI on behalf of and in accordance with the instructions of a PI processor

2.15
privacy
right of a natural person or legal entity or association of persons acting on its own behalf, to determine the degree to which the confidentiality of its personal information (PI) is maintained or disclosed to others

[SOURCE: ISO/IEC 24775:2011]

2.16
processing of PII
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, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction

[SOURCE: EU-Dir 95/48/EC Art 2 lit(b)]

2.17
sensitive data
any personal information related to a natural person revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data or sex life; its processing is prohibited except for closing circumstances

2.18
use of PI
action that circumvents all kinds of operations with the set of PI or certain elements of it meaning both processing of PI and transmission of PI to a third party

2.19
processing PI
collecting, recording, storing, sorting, comparing, modification, interlinking, reproduction, consultation, output, utilisation, committing, blocking, erasure or destruction, disclosure or any kind of operation with PI except the transmission of PI to a third party

2.20
third party
any person or legal entity receiving PI of a data subject other than the data subject itself or the controller or the processor

2.21
transmitting PI
transfer of PI to recipients other than the data subject, the controller or a processor, in particular publishing of data as well as the use of data for another application purpose of the controller

3 Symbols and abbreviated terms

The following abbreviations are common to this document:

APEC	Asia-Pacific Economic Cooperation
Art	Article (clause in an EU Directive or similar document)
C-ITS	Cooperative ITS
CoE	Council of Europe
Dir	Directive (as in EU Directive)
EC	European Council
EU	European Union
ITS	Intelligent Transport Service
OECD	Organization for Economic Co-operation and Development
para	paragraph
PI	Personal Information

RDB relational databases

UN United Nations

VS Video Surveillance

4 Background information

4.1 Historical background

At the time of first codifications of rights (e.g. ancient Hammurabi's-Stone (1770 BC), ancient Grecian Drakon's law (621 BC, codification of existing law, abolition of vendetta), Solon's law reform (593 BC, general discharge of debts, abolition of bonded labour, personal freedom of citizens and structured in four classes), Kleistenes' law reform (507 BC, one homogenous citizen class, extension of political participation), the ancient Roman Twelve-Table-Law (450 BC) and Justinian's Corpus Iuris Civilis (534 AD)) the basic rights of a person like dignity were seldom subject to regulation. The codifications served mainly the written declaration and determination of basic rules for possession and property, related human actions, solving conflicts, the balance of interests between different positions of persons or rights of domination of a sovereign and some criminal law for severe criminal acts.

The first written declaration of freedom rights happened in the "*Magna Carta Libertatum*" on June 15th 1215 AD in England, by which Jonathan Landless (1199 – 1216) granted the Church of England and the nobility some privileges. This document contains additionally (par 39) the freedom for all free citizens. However, this freedom of citizens was in reality performed about some hundred years later. The "*Magna Carta Libertatum*" is valid constitutional law in Great Britten today.

The written rights of freedom of all citizens was confirmed indirectly in the "*Habeas Corpus Act*" (1679) and the possibility of a fair defence of them before a court by the "*Bill of Rights of England*" (1689) which was model for the US Constitution.

The right of freedom and the dignity of a person were intensively discussed during the age of Enlightenment by Montesquieu, Rousseau, Voltaire, d'Alembert and Diderot to mention the best known. However, the sovereigns did not convert their ideas in law, because these ideas would cut back their power.

Nevertheless, these ideas were written down in the "*Virginia Declaration of Rights*" 1776 when the USA was founded. It was followed by the "*United States Bill of Rights*" (1789) and "*Declaration of the Rights of Man and of the Citizens*" at the French Revolution on August 26, 1789. Their performance and distribution is well known.

The following decades during the 19th and 20th centuries were characterized by revolutions and not evolutions of these ideas. However, it is worth mentioning that the Austrian General Civil Code (ABGB) of 1812 in its Clause 16 already declares: "*All human beings have inborn rights convincing by sense and therefore to be considered as a person."* At this time, this clause had constitutional character for the Habsburg Empire and is a central law in the Austrian legal system.

The two World Wars and especially the Nazi Regime forced the General Assembly of the United Nations to proclaim on December 10, 1948 the "*Universal Declaration of Human Rights*". Its Article 1 states:

"All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood."

In 1949, the Federal Republic of Germany followed it in their Basic Law (constitution), of which Article 1 paragraph 1 declares:

"The dignity of man is untouchable. It to respect and to protect is the obligation of all state authority."

In November 1950, the Council of Europe by its Declaration of the “Convention to protect Human Rights and basic Freedom” achieved a further progress. Some states enhanced it to constitutional rights (Austria, Liechtenstein, Norway, Switzerland, and United Kingdom).

The European Charter of Fundamental Rights achieved the last step in the development of the law on this subject. This came into force at December 1st, 2009 and is now immediate applicable right in all European Member States. Article 1 of the Charter uses similar wording to the German Basic Law:

“The dignity of man is untouchable. It is to respect and to protect.”

Article 8 is of special interest for this Technical Report:

“*Protection of personal data*

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.”

It is obviously clear according to the above declarations of constitutional rights and the EU-Charter, that the dignity of man is a central protected value. The protection of personal information is derived as a further value out of dignity. It is protected by precautions like the principle of equal treatment, ban of torture, and the prohibition of discrimination (based on gender, descent, race, language, origin, faith, political opinion, handicap or disability). However, the protection of personal information is not possible by usual means; therefore, new means have been developed for it.

The very fast evolution of the information technology compared to other developments brought up the need to protect personal information and prevent its abuse. The reaction to this was a call for privacy principles which was early formulated by the US Department of Health, Education and Welfare Advisory Committee on Automated Personal Data Systems Report (July 1973). The report defined eight principles “***Fair Information Practice Principles (FIPPs)***”.

This report became the foundation for the US Privacy Act of 1974, which regulates the handling of personal data in US federal government databases. Hessen/Germany, Sweden, Austria and France formulated similar principles in national privacy acts. These legal acts led later on to the international guidelines promulgated by the OECD, the Council of Europe, and the International Labour Organization, the United Nations, the European Union and APEC.

4.2 Legal background

All Member States of the European Union have transformed the EU-Dir 48/95 and 2002/58 and their amendments by Dir 2006/24/EC and Dir 2009/136/EC to their national laws. Therefore, data protection law is harmonized in the EU but is used according to the traditional national law system, which creates differences in the results for the same circumstances. The members of the standardization working groups have to observe these differences.

The international rules are mainly

— the UN Universal Declaration of Human Rights (1948, binding for all member states);

— the European Convention for the Protection of Human Rights and Fundamental Freedoms (1950), now renamed to “*European Convention on Human Rights (ECHR)*” binding for all member states, especially Art 8 for Privacy);

— the OECD Recommendation concerning Protection of Privacy and Transborder Flow of Personal Data (1980, not binding, only recommended);

— the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (28/1/1981 published and entry into force 1/10/1985, binding for the CoE member states);

— the EU-Dir 48/95/EC amended by EU-Dir 1882/2003, EU-Dir 2002/58/EC amended by Dir 2006/24/EC and Dir 2009/136/EC;

— the EU-Charter of Fundamental Rights of the European Union (2000/C 364/01, in force since Dec.1th, 2009 and binding all member states), and

— the APEC Privacy Framework (2005, not binding recommendation).

All these international rules are the basis for the ITS Directive EU Dir 2010/40/EU, Art 10, "*Rules on privacy, security and re-use of information"* which requests*:*

"1. Member States shall ensure that the processing of personal data in the context of the operation of ITS applications and services is carried out in accordance with Union rules protecting fundamental rights and freedoms of individuals, in particular Directive 95/46/EC and Directive 2002/58/EC.

2. In particular, Member States shall ensure that personal data are protected against misuse, including unlawful access, alteration or loss.

3. Without prejudice to paragraph 1, in order to ensure privacy, the use of anonymous data shall be encouraged, where appropriate, for the performance of the ITS applications and services. Without prejudice to Directive 95/46/EC personal data shall only be processed insofar as such processing is necessary for the performance of ITS applications and services.

4. With regard to the application of Directive 95/46/EC and 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.

5. Directive 2003/98/EC shall apply."

This is the legal basis for any work on ITS standards that include the use of personal data and has to be taken in account not only for the development of the standards but also for the implementation of the standards in services and products.

4.3 Fundamental Rights of Data Protection and Privacy

Ten principles for data protection and privacy summarize the fundamental rights. They should be included in the work of development any standards that involve the use of personal data.

The following principles are based on the eight **Fair Information Practice Principles (FIPPs)**[1)] accepted in most parts of the world. In addition, experiences from the past have led to the inclusion of two more principles; the first ("*Avoidance*") and the last principle ("*Deletion*") and the eight principles are enhanced by adding the controller to organizations due to the fact, that not only organizations process data. A further change is the replacement of "*individual*" by "*data subject*" and "*PII*" by *"PI*"

1) Rooted in the United States Department of Health, Education and Welfare's seminal 1973 report entitled Records, Computers and the Rights of Citizens (1973), these principles are at the core of the U.S. Privacy Act of 1974 and are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. A number of private and non-profit organizations have also incorporated these principles into their privacy policies.

In order to truly enhance privacy in the conduct of all IT and ITS-transactions, these 10 principles of Information Practice Principles (TCIPPs) shall be universally and consistently adopted and applied in any system which collects and uses PI from the very beginning up to the deletion of PI when it is no longer needed. The way that PI is processed shall be considered as a chain of commands and not as single commands applied in isolation from each other. **"*Privacy by Design*" should be the dominating principle**. The 10 principles should be a widely accepted framework to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy.

Articulated briefly, the 10 principles of Information Practice Principles (TFIPP) are:

Avoidance: Organizations or the controller should avoid all PI related to a data subject as far as possible, and if avoidance is not possible, the collected data should be anonymised before processing. The collection and usage should be covered by a free consent by the individual or a valid contract with the data subject, or a legal act, or a valid not appealable judgment of an accepted and legally defined court.

Transparency: Organizations or the controller should be transparent and provide notice to the data subject regarding collection, use, dissemination, and maintenance of PI.

Individual Participation: Organizations or the controller should involve the data subject in the process of using PI and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PI. Organizations or the controller should also provide mechanisms for appropriate easy access, information, correction, deletion and redress regarding use of PI.

Purpose Specification: Organizations or the controller should specifically articulate the authority that permits the collection of PI and specifically articulate the purpose or purposes for which the PI is intended to be used and to whom they are disseminated.

Data Minimization: Organizations or the controller should only collect PI that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PI for as long as is necessary to fulfil the specified purpose(s).

Use Limitation: Organizations or the controller should use PI solely for the purpose(s) specified in the notice. Sharing PI should be only for a purpose compatible with the purpose for which the PI was collected.

Data Quality and Integrity: Organizations or the controller should, to the extent practicable, ensure that PI is accurate, relevant, timely, and complete (refer to 5.13).

Security: Organizations or the controller should protect PI (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Accountability and Auditing: Organizations or the controller should be accountable for complying with these principles, providing training to all employees and contractors who use PI, and auditing the actual use of PI to demonstrate compliance with these principles and all applicable privacy protection requirements.

Deletion: Organizations or the controller should delete all or partly PI physically even in all backups after the purpose is achieved and the PI is not needed anymore or retaining and safekeeping is forced by law.

The universal application of these principles provides the basis for confidence and trust in all IT and ITS transactions which include PI.

5 Basic elements of data protection and privacy

5.1 Personal information (PI) and its avoidance

5.1.1 General

EU-Dir 95/48/EC, Art 2 lit. (a) defines personal data and personal information as any information relating to an identified or identifiable person (data subject). Such data or information could be anything as shown in the following figures, which illustrate all the circumstances under which information is left or could be gathered.

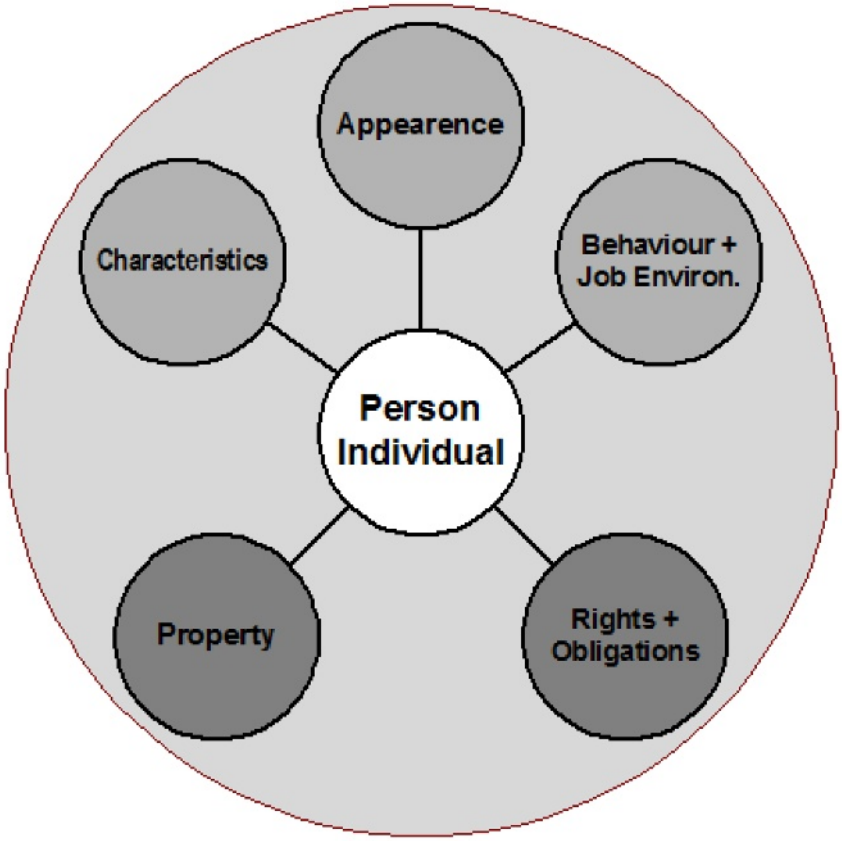

Figure 1 — Personal Information related to a person by personal characteristics

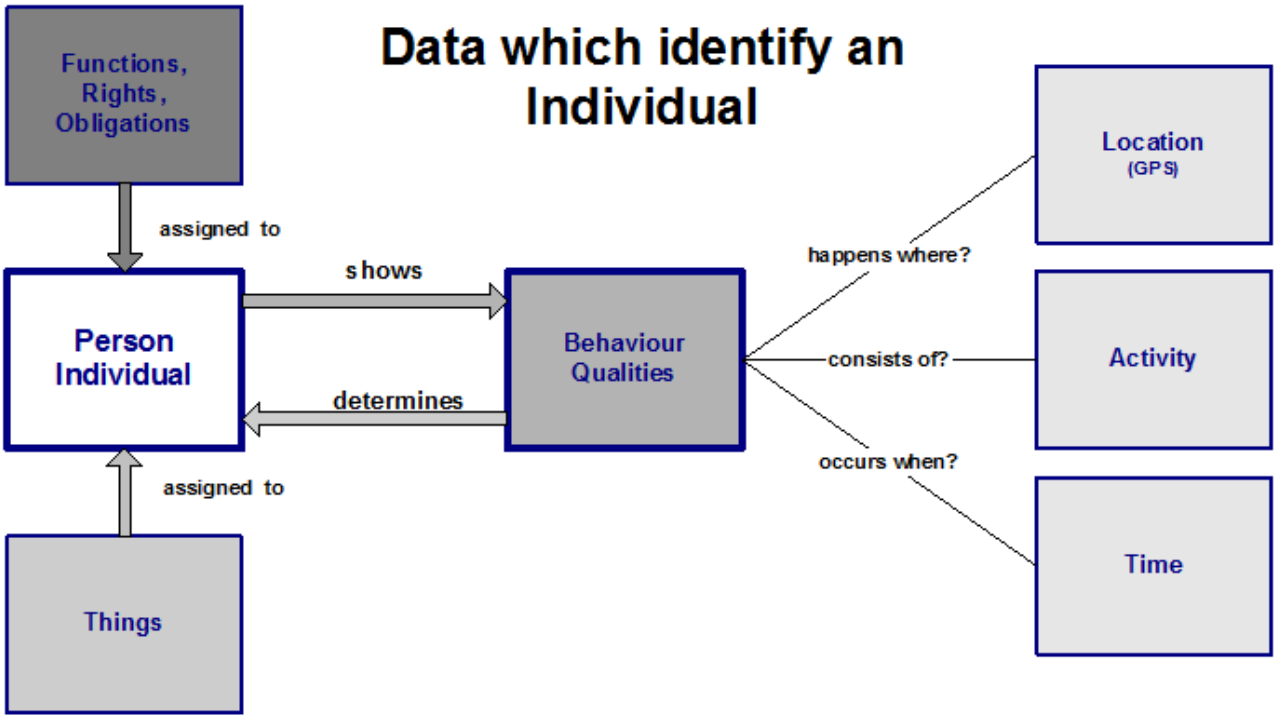

Figure 2 — Personal Information related to behaviour of a person

These two figures overlap but they pinpoint to the different situations where PI is involved. As one can recognize immense possibilities exist for collecting or accessing PI. This means that the avoidance of the use of PI in any ITS related process could be a complicated task. In order to illustrate some attributes that can be used to identify natural persons the following list (taken from ISO/IEC 29100 with some extensions) provides many (but not all) examples of the attributes that can be used to identify a natural person:

1) age or special needs of vulnerable natural persons;

2) allegations of criminal conduct;

3) any information collected during health services;

4) bank account or credit card number;

5) biometric identifier (in the future possible access to the vehicle to start it);

6) biomedical data;

7) credit card statements and numbers;

8) criminal convictions or committed offences;

9) criminal investigation reports;

10) customer number;

11) date of birth;

12) diagnostic health information;

13) disabilities;

14) doctor bills;

15) employees' salaries and human resources files;

16) financial profile;

17) gender;

18) GPS position;

19) GPS trajectories;

20) home address;

21) IP address, if it is static or when dynamic stored for a critical time period;

22) location derived from telecommunications systems (Cell-ID);

23) medical history and data;

24) mobile telephone number(s), if public available;

25) name;

26) national identifiers (e.g. passport number);

27) personal e-mail address;

28) personal identification numbers (PIN) or passwords;

29) personal interests derived from tracking use of internet websites;

30) personal or behavioural profile;

31) personal telephone number;

32) photograph or video identifying a natural person;

33) product and service preferences;

34) racial or ethnic origin;

35) religious or philosophical beliefs;

36) sexual orientation;

37) social security number;

38) trade-union membership;

39) telephone number(s), if public available;

40) utility bills;

41) vehicle license plate number.

Many ITS services and applications (particularly those that support Cooperative-ITS) frequently use the examples of attributes highlighted in bold type. The use of these attributes within ITS services and applications, and in the standards that support them, will require special care.

It is important to mention that as more information or data elements are used by ITS services and applications it becomes easier to identify the person to which they relate. This is despite the fact that this information and data elements at first appear to be unrelated to a person. Modern data mining tools have made it much easier to identify natural persons from publicly available data. This is one reason why gathering and using data that even indirectly points to a person could endanger the privacy of that person. Therefore, the first and most effective principle is to avoid the use of personal related information (PI) as much as possible.

Obviously if PI is not used it cannot be abused or violated, either through negligence or direct action. Not using PI will also save effort and costs for implementing ITS.

5.1.2 GPS-Data or GPS-Trajectories

In ITS, nearly all messages transmitted by vehicles contain geographical data or GPS data elements that are particular to that the vehicle and could be used to identify its driver or owner and as such are possibly PI. The reason for this is that the GPS location of the starting point or end point of any vehicle trajectory may be a special location, which could be the home location or the working place of the driver or the registered user of the vehicle. The location could also be a hospital, a meeting point of political party, a trade union location, a religious assembly or a brothel (all sensitive data according to EU Dir 95/48/EC, Art 8 par 1) which the driver or owner of the vehicle has a legitimate reason to visit.

In order to avoid a possible violation of privacy the starting point or the end of any vehicle trajectory should be smeared by deletion of the last two decimal places of both coordinates (e.g. nnnn.nnnn - > nnnn.nn for latitude and eeee.eeee - > eeee.ee for longitude). This smearing of coordinates extends the smaller radius of the elliptical area of the GPS-coordinates from initial some 5 – 10 m to final 3,3 km (at North Cape) to 9,1 km (Cyprus) which seems enough to delocalize even a single house in a low occupied region.

This smearing of GPS-data are only necessary for start and end points of vehicle trajectories if the time that the vehicle is stationary at either of them exceeds the usual stop time at traffic lights. In this case, the GPS-data for the sequential points on the vehicle trajectory shall not be smeared in order that the expected services can be provided. The same principle should be applied to the situations where vehicles are stationary in traffic queues, although in this instance other factors will need to be taken into account since the "*stop time*" can on occasions be significant parts of hours, rather than seconds. GPS-data for moving vehicles should not be smeared, as this will prevent the implementation of some services, such as those for lane keeping and collision avoidance.

The following example shows the effect of the smearing process:

In Vienna/Austria the famous St. Stephan's Cathedral entrance has the GPS coordinates longitude 16,37266° and latitude 48,208724°. These coordinates define the location on earth with an accuracy of the last decimal place of longitude ± 0,000.005° ≡ 0,741 m and for latitude ± 0,000.000.5 ≡ 0,111m. In order to smear the coordinates to a level of around 100 m the last two decimal places of longitude should be deleted which gives the new longitude of 16,373° and for the new latitude of 48,2087°. This creates an uncertainty around the entrance of the cathedral of ± 37 m longitude and of ± 55,6 m latitude. This uncertainty corresponds to an ellipse of a = 55,6 m for the half axis North–south and b = 37 m half axis East – West. The following Figure 3 shows these two uncertainties by deleted last decimal places.

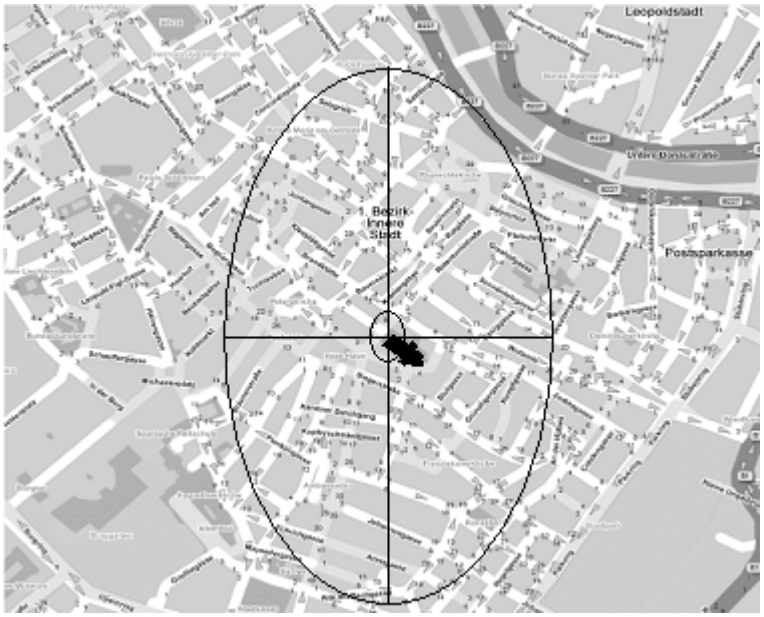

Figure 3 — Vienna St. Stephan Cathedral Entrance and GPS-ellipses (deleted 1 and 2 decimal places)

5.2 Sensitive data

Besides the usual PI such as name, home address and birthday, the EU Dir 95/48/EC defines in Art 8 par 1 some data as being of a special category, and prohibits the processing of it (with some exceptions listed in 5.7). These special categories of data are personal data revealing:

— racial or ethnic origin,

— political opinions,

— religious or philosophical beliefs,

— trade-union membership,

— data concerning health or

— sexual life.

Usually ITS services or applications do not use such data about a person. However, as explained above via the starting or the endpoint of a vehicle trajectory the person could be identified and the location of the starting or the end point could be interpreted as a point, the address of which is related to one of the above special categories. In this case, the starting or the endpoint of a vehicle trajectory becomes sensitive PI data and under the provisions of the EU Directive should not be processed. The ban includes even the storage of such related GPS-Data because of its sensitivity.

5.3 Individual or data subject

The EU Dir 95/48/EC has no specific definition of the individual or data subject, but states in Art 2 lit (a) an identified or identifiable natural person (‘data subject’) to which data are related, is considered as the subject to be protected. It leaves the precise definition of the data subject to be decided by the individual EU-Member States, though some Member States also include **legal entities** and/or associations of persons as needing to be protected. This member states are:

— Austria, due to the fact that legal entities are completely equally treated like natural persons even in trade and civil law;

— Denmark;

— Iceland;

— Italy;

— Luxembourg;

— Norway;

— Switzerland.

In addition, Austria protects associations of persons and, as a special exception, Slovakia even protects the data of deceased persons.

The open question is whether the expected new EU Regulation of data protection grants the protection to legal entities too. This inclusion makes sense but it is a political question.

For the time being, it is recommended that ITS standards should treat legal entities and the association of persons in the same way as natural persons, in order to avoid raising conflicts at national levels in the countries mentioned above.

Most of the international recommendations like APEC or OECD or European Council restrict the protection to natural persons.

The ISO/IEC 29100 "*Privacy Framework*" names the data subject as Principal and defines it as "*natural person to whom the personally identifiable information (PII) relates*".

In ITS services or applications, one has to consider two possible data subjects:

— driver of the vehicle as a natural person and/or

— owner or registered user of the vehicle, which could be a natural person or a legal entity, or an association of persons.

In about 60 −70 % the driver is the owner or registered user of the vehicle. Even when the driver is not the owner, its PI is protected.

5.4 Controller

5.4.1 General

The EU Dir 95/48/EC defines the "*controller*" as the natural or legal person, public authority, agency, or any other body which alone or jointly with others determine the purpose and means of the processing of PI. APEC and the European Council (ETS108) and OECD use similar definitions.

5.4.2 ITS environment

With these definitions, it seems clear who the controller of PI is, but that is not true in ITS-services and applications. The reason for this uncertainty comes from the process chains and definitions in the standards. For instance the ITS-station in a vehicle sends out some vehicle related parameters due to fact that a sensor (e.g. outside temperature sensor) has reached the level where the lane becomes icy. This message and the location are of importance for all following vehicles and the infrastructure to focus the attention of the drivers to this fact and they should carefully pass this location. Who is the controller for this message and takes the responsibility?

The driver or the owner of the vehicle does not even know this process and has not initiated the transmission. One could argue that the vehicle driver or owner gives implicit consent, but for implicit consents special and very strict rules have to be applied to accept its validity. These rules do not apply for this case because although the driver starts the vehicle and because of this the ITS-station starts its functionality, the driver is the data subject and could not be the controller.

In addition, the vehicle manufacturer or after-market equipment provider cannot be considered to be the controller, because it has only assembled the ITS-station in the vehicle.

Usually the message is pseudo-anonymous and as such out of the scope of data protection law by all existing legal systems and recommendations too. However, it could be back traced to the sending vehicle if necessary and if it is possible to gain access to the decryption process and the key. This scenario could be happen for the case that the originating vehicle transmits false parameters due to a faulty sensor or its manipulated ITS-station sends false parameters. By identifying the vehicle transmitting false parameters, the driver or owner is up to certain level identified too, because this faulty behaviour shall be corrected which is only possible by identifying the driver or owner of the vehicle and get access to it.

Similar scenarios could be constructed for other ITS services and applications. The main question for these scenarios is who is responsible for the PI violations or how could be such scenarios be avoided or legally solved. The existing European law does not contain an explicit statement for such scenarios.

A legal salvation of such problems could be found when the definition of the controller is teleological interpreted such that any PI that has been illegally gathered, used and processed is allocated to the user who initiates this process. Such users are **illegal controllers** except for the case where the driver's consent has been given to use the PI data, or they have a legal based reason (by law, by a valid and legally based decision of an administrative authority, or a valid decision of a court, or vital interest of the controller, or for the data subject). They have at least the same responsibility and liability as any legal controller based on data protection law, in addition to their liability in respect to criminal and civil law.

5.5 Processor

Because the controller of PI frequently hands over the processing of the gathered PI to a subcontractor, which has the means to process the handed over PI, not all data protection acts and recommendations define the role of such subcontractors. These subcontractors are usually called “*processors*” and EU-Dir 95/48/EC Art 2-lit (e) define their status by:

“‘*Processor*’ shall mean a natural or legal person, public authority, agency or any other body **which processes personal data on behalf of the controller;**”

APEC, Council of Europe and OECD has not defined the role of “*processors*”. They are more or less part of the controller and seen as its tool.

Considering ITS one can find that processors could be

— part of the ITS infrastructure that process PI in addition to transporting it to any receiver;

— the ITS-station in any vehicle except if it functions only as a relay-station for the transmission of messages between sources and receivers;

— any final receiver of messages that processes the received messages on behalf of the transmitter and then sends it back to the transmitter.

The EU Directive does not define special liabilities for the processor. EU left the definitions of these to its Member States. Most Member States charge processors with the same obligations, responsibilities and liabilities as “*controllers*”.

5.6 Third Party

The controller frequently hands over PI to other persons or organisations for their own interests. This case extends the uncontrolled use of PI and endangers the privacy of the data subject. In order to give the data subject a better control of their PI, EU-Dir 95/48/EC defines in Art 2lit (f):

"'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data."

Therefore, the third party is an independent entity (person, legal entity, organization etc.) that receives PI from the controller and uses it for its own interests.

To avoid any abuse of this PI the controller has to inform the data subject in the initial consent for processing the PI that the data subject allows the controller to transmit the PI to named and addressed third parties for their own interests, but only with all conditions the data subject had explicitly stated in their consent. If no such conditions are stated, the third party has to observe either the usual condition of the data protection law or their published declarations concerning data protection and privacy. The third party shall use the PI in favour of the data subject.

The form of handover of the PI is irrelevant; it could be by hand or electronically or by any other means. It is worth noting that some national laws interpret the handover of the PI inside the controller for another purpose not explained in the consent requested from the data subject as an **invalid purpose**.

The third party could be the public too even when the PI is disclosed to the public by intension or by negligence.

For the transmission of the PI from the controller to a third party it is necessary that the processing of the PI by the controller is legitimate.

An important condition for a legitimate transmission to a third party is that the third party has provided the transmitting controller with sufficient information to show that it has the proper legal responsibility for receiving the PI. Otherwise, the third party is an **illegal controller** and it has the same liability and responsibility as the legitimate controller.

A further important condition is that the third party receives not more PI than is necessary to service its interests. This is an expression of the principle of data minimization.

All these conditions request a carefully negotiation between the controller and the third party about content, utilization, purpose, time limit and timely deletion of PI.

APEC mentions the third party only as possible provider of PI or as legal receiver of PI. European Council Convention and the OECD guide do not even mention the third party as possible user of PI.

5.7 File or filing system (manually or automatically processed)

A file or filing system that contains the PI of data subjects is defined as a structured set of PI. This applies even if the file or filing system is accessible according to specific criteria, if access to it is gained manually or automatically by electronic means, or whether it is centralized, decentralized or dispersed on a functional or geographical basis. This means that for ITS, the possibility of dispersal of all or parts of the PI of any data subject has to be treated in the same manner as the concentrated PI.

5.8 Consent

The valid consent of the data subject in the utilization of its PI requests that the data subject is informed beforehand by a certain, legitimate and unambiguous way about the circumstances and for what purpose its

PI will be used and distributed, plus information about the controller and third parties that will be involved. The consent shall occur without any pressure being applied either explicitly or implicitly for the data subject to accept and as an expressed declaration of intent. Even in civil law this consent, whether as a result of a directly or an implicitly expressed declaration of intent, is only valid if the data subject is legally capable of giving it. The implicit declaration shall express generally accepted actions, which do not leave reasonable doubts even when considering all the circumstances.

The capability to give consent is bound to the legal capacity of the data subject. This capacity is determined by the age and lucidity of the natural person acting for itself or as an agent for a legal entity or organization. For a juvenile the validity of the consent depends on its age and understanding and for a mentally disabled adult additionally its ability to understand the complexity of the circumstances of the case. The "*bona fide*" rights protection for consent for the controller of the PI is invalid for juveniles and mentally disabled persons due to the legal protection of such persons. Therefore, the controller could not trust in the bona fide right for such persons.

The coverage of the consent is very critical. In order to get a valid consent the controller of the PI needs to make it transparently obvious to the data subject that it collects the PI of the data subject for specific and legitimate purposes and the controller does not retain the PI in a way that is incompatible with those purposes. For scientific and statistical purposes, there exist some reliefs. The controller has to reveal to the data subject that

— it will use the PI fairly and lawfully and

— only use PI insofar as the PI is essential for that purpose and

— the utilization is not excessive in relation to the purpose and

— the PI will be used so that the results are factually correct with regard to the purpose of the application and

— the PI will be kept in a form which permits identification of the data subject as long as this is necessary for the purpose for which the PI is collected and

— the particular laws concerning archives request longer period of storage will be applied.

The controller bears the responsibility for ensuring that all data applications comply with these principles and they apply too when a processor is employed to use the PI. These rules are part of the transparency requirement.

It shall be remembered that the consent of the data subject is a strictly personal right. This means that an agent on behalf of the data subject could not provide the consent. The data subjects have to provide it only by themselves.

A further condition on the validity of the consent is that it has to be free of any pressure or obligation on the data subject. This means that coupling the consent to any necessary service for the data subject makes the consent invalid because it is not free of pressure or obligation. This is a fact that has an important impact on ITS and C-ITS.

For example, the driver or owner of a vehicle starts its engine and therefore the installed and incorporated ITS-station starts up. In its start-up the ITS-station immediately starts its services and applications and possibly transmits some messages containing the PI (for instance the vehicle is leaving a parking area). The starting of the engine could not be interpreted as a valid consent to transmit the PI to the controller (operator of the parking area), because it is unavoidably coupled with the start of the engine and probably unconscious to the driver or owner.

A further problem arises if the vehicle belongs to a company and the company uses the collected data of the vehicle to supervise the driver. This way of working is prohibited by law in some EU Member States (for instance in Austria and Germany) because such supervision affects the dignity and privacy of the driver.

5.9 Withdrawal of consent

EU-Dir 95/46/EC, Art 14 gives the data subject the explicit right to oppose the further processing of its PI even when the PI are legitimately collected and processed and the data subject had consented. This right shows clearly that the data subject is the principal of his data. The revocation means that further use and processing of the PI is not allowed.

The revocation is invalid for the case when the PI is necessary for the controller or its agent to fulfil a contract for which the PI is collected and processed. Otherwise, this revocation leads to a unilateral cancelation of the related contract. It is invalid too for any PI that is necessary for the enforcement of valid claims in a process before an administration or a court.

The revocation is also invalid for parts of PI that exist independently of the data subject, but for which the link between such data and the data subject has been broken and deleted.

Any PI that has been collected and processed based on law or a legitimate decision of an administration or court cannot be revoked.

5.10 Fairness and legitimacy

EU-Dir 95/48/EC, Art 6 par 1 states that controller has to use the PI in a fair and legitimate way. This means that the controller has to be fair and honest in its processing of the PI and even does not negligently hide from the data subject the collection and processing of its PI.

Legitimacy means that the collection and processing of the PI is based on

— the free and valid consent of the data subject or on

— a valid contract with the data subject or

— a valid law or

— an un-appealable decision (res judicata) of the responsible administration or court or

— vital interests of the data subject or another individual request the application of the PI.

These five reasons are equivalent to the meaning of legitimate.

5.11 Determination of purpose

Art 6 par 1-lit (b) states that the PI should only be used if

"*collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguard;*"

This statement expresses the strong binding of the use of the PI to the revealed purpose. The careful interpretation of the statement leads to the inclusion of transmission of the PI or its disclosure to a third party in what can be considered part of the purpose, plus the use of it for a purpose not disclosed to the data subject. If the PI is not collected and processed legally then its transmissions or disclosure to a third party is illegal and the use of such a PI by the third party illegal too. The collection and processing of sensitive PI is absolutely prohibited. If such PI is unintentionally collected and processed, and the controller subsequently

recognizes this has happened, then the controller has to delete immediately such a PI or if possible delete at least the sensitive part of the PI in order to make the PI no longer sensitive. The reason for such a task is the lack of consent for collection and processing of such a PI.

5.12 Minimization of PI

EU-Dir 95/48/EC, Art 6 par 1 lit (c) states that PI may only be used as far as they are

"adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed."

In order to achieve this request it is necessary to try to minimize the demand for the PI's of a data subject as much as possible. Thinking in conventional ways does not solve this request. The thoughts should always be about a creating system, service or product, which does not use any PI because it will cost a lot less to develop and operate. Development of such systems, services and products may need the investment of a little more in research and development but by the financial benefit should be much more than the investment. This principle in development is now called "***Privacy by Design***" and is the best for society and the individuals. It is also valid for the development of the standards that build the framework of services and products and enables the implementation of the basic rules enshrined in many national constitutions and charters.

It is obvious that the total avoidance of PI cannot be included for some specific services, such as when a contract is necessary between partners. In such cases, the rules described previously in the Technical Report for the use of PI should be followed.

Directive 95/48/EC Art 17 demands that

"the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing."

It is obvious that the fulfilment of this demand is not free of charge. Therefore, the minimization of PI is not harassment but a reasonable goal, because it reduces costs and risks.

5.13 Topicality and correctness of PI

EU-Dir 95/48/EC Art 6 par 1-lit (d) states that PI shall be

"accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified";

Adhering to these principles of topicality and correctness of PI means:

— ensuring the process of collection of PI includes requests that they are accurate, complete, up-to-date, adequate and relevant for the purpose of use;

— ensuring the reliability of PI collected from a source other than from the data subject itself or transmitted to the controller by a third party, before it is processed;

— establishing adequate control procedures to periodically check the accuracy and quality of the collected and stored PI;

— verifying, by appropriate means, the validity and correctness of claims made by the data subject prior to the performance of any changes to PI in order to ensure authorized changes.

It is obvious that incorrect PI's create not only trouble and possibly harm to the data subject but has adverse effects to the controller too. Therefore, the use of PI's is not only a problem of collection but also the organisational effort to handle it appropriately. In addition, use of PI's causes extra costs and binds resources during the time of their use and processing. Avoiding the use of PI's saves all of these.

5.14 Time limits to PI

Collected PI's are usually retained and stored for intentionally later use. However, EU-Dir 95/48/EC Art 6 par 1-lit (e) states that PI is

"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed."

Therefore, PI's should not be stored and kept in stock for possibly later use. The controller has to physically delete each PI after its data has been processed to fulfil the purpose for which it was collected. It is very important to note that simple logical deletion is not enough as several decisions from national supreme courts have requested the physical deletion of PI's in a way that they could not recovered by any means. Even blocking a PI is not enough because someone could still gain access to it.

This creates a special problem in modern relational databases (RDB) because they are usually prepared for tax and trade law, which do not allow deletion of a record but only mark it as invalid and supplement it by a correct record. The break-up of the index in the RDB is not enough because it removes the PI or data element only from the RDB but it is still on the storage device and is not deleted. Special mechanisms will be needed to solve this problem for RDBs in order to conform to the law.

When a database, which contains PI, is being designed, the PI elements should have a delete date in order to fulfil the requirement of the time limit, so that the PI is automatically deleted if its purpose or a condition is fulfilled. This concept is part of the principle "***Privacy by Design*"**.

It is expected that the revision of the General Data Protection Regulation that the European Commission plans to introduce, will include the "***Right to Forget***", which will come into force after a to be defined time. Taking this into account it is recommended that the early deletion of PI's is included in new standards and replaces the current practice of keeping PI's as long as possible irrespective of the law.

5.15 Security requirements to PI

The whole data protection principles are useless if the controller and its processor do not protect the PI against abuse and negligence. EU Dir 95/48/EC Art 17 requests in a vary abstract but comprehensive way that:

"the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."

The ISO/IEC standards 27001 – 27005 have included these rules, which describe the processes, their conversion and control in detail. In order to satisfy the demands it is necessary to check how and by what means in the area of information technology the security of the PI and the processing of it could be protected against internal and external abuse, negligence and unintended and unforeseeable incidents like burglary, fire, water, lightning, and faults of power supply.

This protection is not part of this Technical Report but the user of it should consider these events at a very early stage in the development of a service, application or standard in order to perform Privacy by Design.

5.16 Obligation to keep PI secret

The obligation just described in 5.15 (Security requirements to PI) needs to be supported by the obligation of the employees to keep secret the processed PI of all data subjects. EU-Dir 95/48/EC Art 16 fixes this liability through the following statement.

"*Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data, must not process them except on instructions from the controller, unless he is required to do so by law.*"

Law already states this liability and it should additionally be part of a contract commitment of employees that work for a controller and/or processor dealing with PI's.

The problem with such commitments is that they are regularly signed by the employees but in the course of time forgotten and then violated by negligence. In order to avoid such negligence it is recommended that these commitments are reinitialized whenever a significant change in the working situation or field of activity takes place.

The commitment should be by writing for the employee and the employer and should be stored. To support the commitment, the employees should be regularly trained in the results of the newest and practical experiences of data security. These anchor the commitment and correct behaviour for a long time.

5.17 Obligation to inform the data subject (Individual or legal entity)

The data subject has no knowledge of its rights when it does not know about the collection and processing of its PI. In order to give it the chance to be informed about who collects and processes its PI, EU-Dir 95/48/EC Art 18 – 21 and all other recommendations say either the following or something similar to it:

"the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes."

Additionally and accordingly to Art 10 the data subject itself has to be informed about the collection of its PI when it is not collected directly from the data subject but from a third party and processed. This may be based on exemption laws or the interests of an independent third party in order to protect their legitimate interests.

The data subject has a further right to be informed about an intended processing of its PI in the situation where it has the right to object this data processing because it violates its special interests. It is also necessary to inform the data subject when it is not clear whether or not it is obliged to answer questions or when its PI is to be processed in an "***information compound system***". The Directive does not describe explicitly what such "***information compound systems***" might be. For example, the "***Schengen Information System*****"** is a legitimate information compound system based on the treaty of its member states.

However, the most important obligation to inform the data subject arises when a systematic or severe violation of PI has happened and the data subject could threaten harm. This obligation does not take place if the threatening harm is obviously negligible or the effort to inform all affected data subjects is significantly higher than the damage to them.

The need to inform the data subject could be dropped if the PI stems not from the data subject but from another activity of the controller or from a transmission of data from other controllers and

— the application of PI is foreseen by law or by ordinance or

— it is impossible to inform the data subject due to its inaccessibility or

— in view of improbability of an infringement of the rights of the data subject on the one hand and the costs of informing all data subjects on the other hand, requires an unreasonable effort.

5.18 Right (access) to PI

EU-Dir 95/48/EC Art 12 lit (a) states that every data subject has the right to obtain from the controller without constraint at reasonable intervals and without excessive delay or expense:

— "confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

— communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

— knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1)"

This right to access is extensive and complicated because some additional conditions have to be observed which are not explicitly expressed in the Directive but are interpreted in favour of the data subject by the courts.

One condition is that the controller shall answer in writing to every inquiry even in the case that the controller has not collected and processed any PI from the inquiring data subject. This "***Negative Response***" is **mandatory** and for the first inquiry per year needs to be made at no cost to the entity making the enquiry. The reason for this obligation is that the data subject has otherwise no chance to find out whether or not any controller has collected and processed any PI about it. This information is needed by the data subject in order to submit any claim to the supervising authority.

A little more complex is the provision of evidence of identity by the data subject. This obligation on the data subject is obvious because otherwise any person or entity could fake the identity of the data subject and could thus get access to the PI of the data subject. In order to fulfil this obligation for both the inquiring data subject and the inquired controller the evidence has to be based on a certified valid document e.g. passport or any similar document issued by the related authority. The reason for this complex process is to ensure that only the correct data subject is able to get the answer from the controller. Even an agent like an employed lawyer has no right to receive the response of the controller. Therefore, the mail carrier shall personally hand out the written response to the data subject, which then signs the acknowledgement of receipt. No processes, which bypass this approach, fulfil the protection of the PI. For the data subject it means some effort has to be made but it is justified by the obligation of the data subject to assist the inquiry (according to Art 11, which restricts the right of the data subject if too much the effort will need to be provided by the controller).

It is also obvious that the data subject could not abuse its rights by frequent inquiries. For such cases, the controller has the right to obtain compensation for its effort to respond to the inquiries.

The response has to include all stored and processed data and needs to be presented in clear and comprehensive form. Therefore, as a minimum the response should contain:

— the collected and processed data;

— any information about its origin;

— any information about the receiver of the data or receiver groups (third parties);

— the purpose of processing the data;

— the law on which the processing is based.

The origin of the data are necessary in order to give the data subject the chance to find out the identity of the initial controller, which collects the PI. It also enables the data subject to inquire the controller what further

receivers (if any) will see its PI, the purpose for which the initial controller and any further receivers has collected the PI, and the basis in law for their processing of the collected PI.

The response period for the response is allowed to vary between some weeks to some months, but is usually less the 2 months.

For some legal cases, the controller has the right to refuse to provide detailed information in response to the inquiry from the data subject. However, the controller needs to give a written response containing the reasons for refusal to provide a complete or incomplete response.

The controller has to organize its internal process for responding the inquiry in such a way that it has to store the actual PI for a certain time in order that it could prove the correctness of the response when the data subject lodges a complaint against the controller to the supervising authority about the response. This period depends on some deadlines for such complaints, which differs per Member State and the workload of the supervising authority. During this period, the controller shall not delete or manipulate the PI because it could be part of evidence before the supervising authority or court.

For the case the data subject has directed its inquiry to the processor or a sub-processor than the processor or the sub-processor are obliged to inform the data subject about the controller that provided the PI from the data subject and its contact details. This is to enable the data subject to redirect its inquiry the right controller, which will need to be done in a given period.

5.19 Right to rectification and erasure of PI

EU-Dir 95/48/EC Art 12-lit (b) gives the data subject the right to request rectification and erasure of incomplete or incorrect data in its PI. The obligation to make this change to the PI, which will have been processed against law and the right to request the deletion of it, has to be carried by the controller for the instances when:

— it has knowledge about their incorrectness or the illegality of their processing or

— the data subject has proposed a reasonable request.

The controller has to inform the third parties that received the PI from it so that they can perform the same rectifications and deletions to the PI. The third party has the same responsibility and liability as the controller.

The publication of any PI creates a problem if the receiver of the PI could not be determined. Clause 5.17 already explains that the effort to inform the data subject has to be in a reasonable relation to the harm that would be caused if the data subjects are not informed. This restricts the obligation.

The proportion and kind of rectification that will be needed depends on the correctness and status of the PI and it is closely related to these principles.

The controller needs to prove the correctness and status of the PI except if the PI is directly collected from the data subject and with its consent. This means that the data subject has to justify the incorrectness and the wrongfulness of its PI. However, the controller has to prove the contrary.

The purpose of any documentation (based on law or important interests of a third party) excludes any rectification and prohibits any successive change. A comment about this PI rectifies this.

The controller rectifies it in a certain period and informs the data subject about it or gives reason(s) why the rectification could not be performed.

If the controller uses the PI of which either its correctness or incorrectness could not be proved then the data subject could request a disclaimer associated to it. Only the consent of the data subject provides the right to remove this disclaimer.

Due to the fact that electronic data are very easy to copy and cheap to store, every IT manager may feel tempted to keep data as long as possible with the ulterior motive eventually it could be used. This motive normally sounds reasonable but it is very wrong for the PI. The danger stems from the fact that the PI could become outdated and the long storage time increases the danger of abuse, negligent use and false interpretation, any of which could harm the data subject. Therefore, the Directive provides the time limit for storing the PI after the purpose of its collection is fulfilled. After that time limit, the controller needs to delete the PI physically and completely in order to prohibit any access to it by any means.

The planned new General Data Protection Regulation of the European Commission with the "***Right to forget***" stresses this obligation of the controller to delete unused and unnecessary PI's. The experience of the past 18 years and from the use of the Internet is the basis for this new planned right.

Because electronically stored and processed data could be deleted by a simple faulty touch of a button it is a standard practice in IT that the used and stored data are additionally stored on a separate device called a backup. Usually special programs and part of the operating system automate this backup procedure. The effect of this automatism is that the user or operator of the IT system does not even know where certain data are stored on the backup device. The consequence is that it is a complex procedure to find the PI's that need to be deleted on the backup device and usually they remain in the system. The proverb "***Never touch a backup!***" expresses this attitude and creates unnecessary danger for PI, which is contrary to the provisions of the law. However, the controller has the responsibility to organize its processing of PI's in such a way that the obliged erasure of PI's really takes place on all devices including those providing backup in a short time frame otherwise it has to take the liability for all failures based on this faulty process.

5.20 Right to objection

EU-Dir 95/48/EC Art 14 grants the data subject the right:

a) "*at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;*

b) *to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.*"

Article 7 already forbids the use of the PI in a way that violates the observance of secrecy of the data subject, if the above conditions are violated. The right of objection takes care of the case that the use of the PI is generally allowed but in contrary to the interests of the data subject. This needs careful consideration of the interests of the data subject and its special situation but in its favour. If the balance is for the data subject rather than the use and processing of its PI then this has to be stopped immediately and the PI physically deleted.

This situation happens only when the controller has not taken the PI from the data subject directly but from a third party or from official sources. Therefore, the data subject has actively to object but the controller is not obliged to give reason for the collection of the PI.

No objection is possible against collection and processing of PI's ordered by law, but objection to the legitimate collection and processing of PI's such as address lists and e-mail-lists is allowed. However, the objection by the data subject to the incorporation of the PI is effective, especially if it includes information about the credit standing of the data subject. This is a very critical application because incorrect data could affect the ability of the data subject to obtain credit and because the suppliers of such data have only their own interests in mind, which could be in general wrong. Such lists of credit standing have to be notified to the supervising authority. However, this notification does not release the controller from its obligation to inform the data subject about the incorporation of the PI in the list.

5.21 Video surveillance (VS)

In ITS video surveillance (VS) is frequently used as a mechanism for collecting data about the movement of people, goods and vehicles through transport networks. The impact of data protection depends on the resolution of the camera and its colour capability. If only a black and white and low-resolution video camera is used and not recorded (only real time VS) then the danger of an impact on data protection is low because the collection and processing of PI is unlikely. Such VS is used mainly for traffic flow observation and similar applications.

Because digital video cameras with high resolution and colour capability have become cheap to buy, operate and install, the application of such cameras has grown significantly, as has the recording of the video images on devices for the same reasons. This has a great impact on data protection because the collection and video processing of the images is easy and effective. Typical applications of this technology in ITS are the reading and recording of vehicle license plates, access control to geographic areas, parts of the road network, and locations used by travellers and/or goods, VS of these location, VS of critical working processes, VS of employees, etc. The danger arises from the storage of the images and subsequent evaluation by special software in order to detect and recognize persons and/or their behaviour so that evidence can be collected of criminal acts or acts explicitly forbidden by contracts and similar reasoned applications. Some of it may be legitimate; however, it depends on the intrusion into the private sphere of the person or entity and the collection of any data that are not necessary for such observations.

For instance with such high resolution colour cameras sensitive data are collected even though this is forbidden by EU-Dir 95/48/EC Art 8, although there are some special exceptions that are not of interest for most applications.

This possibility of violation of the ban of collection of sensitive data has to be taken into account for all VS applications in ITS. It is recommended that the use of such VS is avoided as far as it is possible. If it is unavoidable by some special conditions then the processing should be kept as small as possible and the original data deleted as soon as possible. Only the processed data should be kept according to the important consideration that it is not sensitive and not related to any particular data subject.

For instance, the vehicle license plate number is a PI due to EU-Dir 95/48/EC Art 2 lit (a). An important decision of the German Supreme Constitutional Court forbids the collection of number plate data in order to possibly provide information about the locations and movements of criminal persons. The decision forbids the general collection of license plate numbers because the intention to uncover and prosecute such criminal persons by observation of all licence plates is a violation of basic rights as it casts suspicion on the owners and drivers of all the vehicles carrying number plates.

5.22 Shift in the burden of proof

The basic rule of all evidence is that the one who states a fact or circumstance is the one that has to prove that they are correct. This means the correct certificates or documents need to be delivered or their existence and contents provide by inspection to demonstrate the facts or circumstances in a way that the judge or the decision-making body is convinced. However, this is in practise very hard or near impossible with the consequence that the stated facts or circumstances are true but it cannot be proved.

In order to avoid such a condition, which could be unfair for a harmed and injured party, the legislative orders for such cases require that the burden of proof be shifted to the violator, or to the entity that is more able to provide the proof.

In all IT processes, this entity is the controller of the process because it is impossible for an external person to know and analyse the applied hardware and software, the organisational structure in which the process takes place and practices of the controller without any deep access to all such things. The justification of trade secrets usually prohibits this access. Considering this, it is clear and reasonable that the controller of the IT or ITS service or product has to prove that the hardware, software and processes used to provide it are not faulty. Even if they are faulty, the controller is not liable when it has taken all reasonable acts to maintain all parts and updated it and corrected it whenever a fault or disturbance has been found to have occurred. In

other words there is no liability if it was not possible under practical circumstances for the controller to foresee that a fault could emerges that could harm or violate a data subject. This exception from liability is called "*adequacy*" and means that under normal circumstances for not expectable causal connections no liability takes place. However, it is necessary to be careful and be aware that special expertise demands a much better overview and tracking of causal connections than would be needed from an entity with less expertise.

Considering this, the rules of EU-Dir 95/48/EC, Art 17 need to be carefully implemented and maintained in order to comply with the need for the controller to prove that negligence has not taken place. Neglecting these rules makes the controller responsible and liable for all harms and damages caused by this negligence and by any negligence on the part of its employees plus malfunction of its equipment and systems.

Annex A
(informative)

Examples of the principle of "cumulative interpretation"

If several articles of EU Directive 95/46/EC and the *AEC Privacy Framework* are compared, a "cumulative implication" about the use of data and the purposes for which it might be used can be seen. The example used in this annex is EU Directive 95/46/EC. However, the principle of "*cumulative interpretation*" is just as applicable to the clauses of the *APEC Privacy Framework* or the OECD Guidelines. However, EU Directive 95/46/EC has stronger legal requirement in Europe.

The preamble to EU Directive 95/46/EC states:

"*Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason,* ***the approximation of those laws must not result in any lessening of the protection they afford*** *but must, on the contrary, seek to ensure a high level of protection in the Community*"; (highlighted in bold in this Technical Report).

The fundamental rights and freedoms of a person have therefore to be defined from two viewpoints:

— the view of the person or data subject;

— the view from the outside.

This can be interpreted to mean that the rights and the freedoms of a person are extendable or limited to the point at which they affect the freedoms of others. At this point of interference there has to be a weighting of the freedoms and rights of third parties. However, this is not well defined in any documentation, but will eventually be resolved in the courts. The objective of this Technical Report is to try and help those involve in creating ITS services, applications and standards to avoid these situations in the first place.

If a person has given higher weight to his/her interests and rights compared to the interests and rights of another, then the rights of that person should take precedence. This interpretation is supported by the phrase in EU Directive 95/46/EC: "*the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community*".

EU Directive 95/46/EC, Clause 31 states: "*Whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;*"

An "*interest which is essential for the data subject's life*" can only be derived from the standpoint of the subject of the data and not from the standpoint of the controller.

The preamble to Clause 31 states:

"*Whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person,* ***any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself;*** *whereas Member States may nevertheless lay down national provisions to the contrary;*" (highlighted in bold in this Technical Report).

This restriction of processing data again supports the view that data can only be collected for the benefit of and in favour of the subject of the data.

However, the statement "*whereas Member States may nevertheless lay down national provisions to the contrary*" is potentially contradictory. Working Party 29 (WP29, this body has been implemented by EU Directive 95/46/EC Article 29 in order to supervise the national authorities and owns the authority to interpret the directive beside the European Court of Justice) has been asked to make a ruling on whether a Member State may pass domestic legislation specifically designed to overrule the rights provided by the Directive, or whether this statement only applies to national legislation for a different purpose which can impact on the rights of the individual for issues of overriding precedence, for example national security.

EU Directive 95/46/EC Article 2 (h) states: "*the data subject's consent' shall mean 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*".

This also implies interpretation in favour of the data subject. It can be combined with: "*The purposes for which personal data are collected shall be determined at the time of the collection of the data and shall be explicit and legitimate at the time of collection of the data and use of the data limited to the fulfilment of those purposes*", which is taken from OECD and codified in Article 11 of the Directive.

The implication of the two clauses is more powerful than the import of each of the specific clauses individually. It implies the preclusion of the use of data collected for purpose a) or purpose b), without the express consent of the person who is the subject of the data and requires not only active consent, but also permission given at the time of, or prior to, data collection. The consent should also be truly optional. Therefore, the use of data such as vehicle owner databases belonging to vehicle manufacturers, dealers and servicing entities, or vehicle registration databases belonging to vehicle licensing/registration authorities is very limited.

Article 7 (f) states: "*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).*****"** (Highlighted in bold in this Technical Report).

The last part of the sentence restricts the rights of the controller or third parties. The interests of the controller or any third party are clearly restricted by the fundamental rights and freedoms of the data subject. This again provides strong support of the interpretation in favour of the data subject.

Article 10 states: "*the controller or his representative must provide a data subject from whom data relating to himself are collected*" (with a list of specific information about the controller).

Article 11 states: "*Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed* ***provide the data subject with at least the following information,*** *except where he already has it:*

a) the identity of the controller and his representative, if any;

b) the purposes of the processing;

c) any further information such as:

- *the categories of data concerned,*
- *the recipients or categories of recipients,*
- *the existence of the right of access to and the right to rectify the data concerning him.*

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject." (Highlighted in bold in this Technical Report).

Articles 10 and 11 define the data subject's right to information and correction and deletion of the data if his data are processed. These are again strong indications of the interpretation in favour to the data subject.

Article 13, par 2 states: "*Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.*".

The phrase: "*… in particular that the data are not used for taking measures or decisions regarding any particular individual*" is a technical measure of restraint in the use of data, but again can be interpreted as strong indications of the interpretation in favour of the data subject.

The phrase: "... *where there is clearly no risk of breaching the privacy of the data subject*" is a restriction of the view and interests of the controller or any third party interested in the processing of personal data.

It is not the intention of this Technical Report to suggest that privacy requirements for ITS services, applications and standards should be extended beyond the existing legal requirements or guidelines. However, the advice is that the principle of "*cumulative interpretation of multiple recommendations*" is a legal implication that should be taken into account. This issue is raised in the provision of guidance, in respect of privacy aspects to be considered in ITS services, applications and standards, as they can appear in court decisions and national legislation. In terms of the example given in this annex, in the Austrian Data Protection Act, this cumulative interpretation rule is more strongly expressed by the wording "*überwiegende Interessen*" which means vast (or greater) interest (of the person who is the subject of the data).

Developers of ITS services, applications and standards should therefore consider not only the individual recommendations or requirements, but also the combination of recommendations or requirements and the implications of a consistent view of the specific purpose and use of data concerning privacy. All standards development and system implementation design should take into account, not only the individual recommendations or requirements, but also the effect of cumulative interpretation.

Annex B
(informative)

Data privacy Framework, Directives and Guidelines

- UN Universal Declaration of Human Rights (1948), http://www.un.org/en/documents/udhr/index.shtml
- European Convention for the Protection of Human Rights and Fundamental Freedom (ECHR)1950, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=005&CM=8&DF=15/03/2013&CL=ENG
- OECD Recommendation of the council concerning Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data (23 September 1980 – C(80)58/Final)
- European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No.: 108, 1981 http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=8&DF=15/03/2013&CL=ENG
- 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. 1995, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:NOT
- 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 (Directive on privacy and electronic communications) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:PDF
- Charter of Fundamental Rights of the European Union (2000/C 364/01) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012P/TXT:EN:NOT
- 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 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:207:0001:0013:EN:PDF
- APEC Privacy Framework (2005, **ISBN:** 981-05-4471-5,) http://publications.apec.org/publication-detail.php?pub_id=390
- ISO 24100, *Privacy — The basic principles for probe personal data protection*
- ISO/TR 12859:2009, *Intelligent transport systems — System architecture — Privacy aspects in ITS standards and systems*
- ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy Framework*

Annex C
(informative)

Security related International Standards

— ISO/IEC 13335-1, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

— ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

— ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

— ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security management*

— ISO/IEC 27003, *Information technology — Security techniques — Information security management system implementation guidance*

— ISO/IEC 27004, *Information technology — Security techniques — Information security management — Measurement*

— ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

— ISO/IEC 27006, *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*

— NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™