TECHNICAL REPORT

ISO/TR 12859

First edition
2009-06-01

Intelligent transport systems — System architecture — Privacy aspects in ITS standards and systems

Systèmes intelligents de transport — Architecture de système — Aspects privés dans les normes et les systèmes SIT

Reference number
ISO/TR 12859:2009(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

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

ISO/TR 12859 was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

Introduction

Intelligent transport systems (ITS) are intrinsically linked to the movement and exchange of data. Some of these data are purely situational or anonymous, however several, either by themselves or as part of multiple data concepts, which independently can be purely situational or anonymous, taken together can provide personal information.

In the modern world, it is often neither possible nor desirable for information to always be anonymous, therefore, the privacy of data is protected around the world by data privacy and data protection regulations.

While the evolution and development of ITS technology provides many opportunities for the provision of increasingly sophisticated ITS services mostly designed for the benefit of users, when designing ITS systems and standards it is imperative that, as part of the fundamental design, the legal and moral requirements for the privacy and protection of data be taken into account at an early stage of system design. This is not only desirable from a moral point of view, but is required in order for a system or standard to be legally compliant. This means taking into consideration not only the potential use, but also protection against misuse of data in a system.

Specific data privacy protection legislation is generally achieved through national legislation and this varies from country to country. The general principles are geographically common, however, and due to provisions made by trading blocks such as the European Union and APEC, there are many universal aspects to data privacy and data protection.

Users tend to interpret these guidelines in the context of their national laws. For users in EU member states, *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* and its successive instruments are mandatory within these states. International courts are likely to give precedence to a combination of the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines) and either Directive 95/46/EC or the *APEC Privacy Framework*, as appropriate.

Using the guidelines espoused by Directive 95/46/EC, the *APEC Privacy Framework* and the OECD Guidelines, this Technical Report provides guidance to developers of ITS standards and systems on general data privacy and protection aspects for the fundamental architecture and design of all ITS standards, systems and implementations.

Intelligent transport systems — System architecture — Privacy aspects in ITS standards and systems

1 Scope

This Technical Report gives general guidelines to developers of intelligent transport systems (ITS) standards and systems on data privacy aspects and associated legislative requirements for the development and revision of ITS standards and systems.

For guidance on specific data protection and data privacy requirements on the subject of ITS probe data, see ISO 24100[1)].

2 Terms, definitions and abbreviated terms

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

2.1 Terms and definitions

2.1.1
accountability
responsibility for complying with measures, making compliance evident, and the associated required disclosures

2.1.2
collection limitation
limit to the collection of personal data

2.1.3
data protection
use of means such as legal safeguards to prevent the misuse of information stored on computers, particularly information about individual people

2.1.4
data quality
standard of acceptability of accuracy of personal data

2.1.5
individual participation
right of an individual to have access to personal data held about the individual and the ability to challenge and correct such data

2.1.6
openness
policy of openness about developments, practices and policies with respect to personal data

1) To be published.

2.1.7
personal data
data about a living individual, identified or identifiable, as determined by the privacy laws and conventions of a political jurisdiction

2.1.8
personal information controller
entity or organization that controls the collection, holding, processing or use of personal information

2.1.9
privacy
quality of being secluded from the presence or view of others

2.1.10
purpose specification
purpose for which personal data are collected

2.1.11
security safeguard
safeguard against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data

2.1.12
use limitation
limit to the purposes for which personal data can be used

2.2 Abbreviated terms

APEC Asia-Pacific Economic Cooperation

NOTE This is the group of Pacific Rim countries that meet with the purpose of improving economic and political ties.

OECD Organisation for Economic Co-operation and Development

NOTE This organization promotes stable economic growth in its member states and provides advice to other countries.

EU European Union

NOTE This is the union with economic, monetary and political ties and intergovernmental coordination of foreign and security policies among 27 European member states.

3 Background

3.1 Origin and basis of this Technical Report

This Technical Report originated from discussions in ISO/TC 204 and CEN TC 278, subsequent to legal studies undertaken in Austria concerning the use of personal data in ITS. The pressure for business case justification initially sustains such developments without a clear legal position and it is necessary to consider the technical and engineering possibilities, as well as ensure that they evolve within a framework of generally (internationally) accepted data protection principles and of course within national data protection legislation.

This Technical Report attempts to create the necessary nexus for intelligent infrastructure systems and provide for their implementation to the greatest extent possible. It attempts to serve as a scientifically based study and a practical handbook. It includes the consideration of a representative selection of technical “scenarios”, as well as a comprehensive and detailed account of the most important applicable legal areas.

There are now data privacy and data protection laws in most countries, therefore it is not possible to take every provision in each country into account. Rather, the recommendations of this Technical Report provide general guidelines which the user should use for general guidance within the context of the national legislation of an implementation (which takes precedence). Developers of standards should test the basic architecture and concept design of their standards against the recommendations in this Technical Report. For an example of national implementation of guidelines, see Annex B.

The recommendations in Clause 4 take the form of a checklist of features to be consulted when developing a standard or an implementation. This Technical Report does not attempt to interpret the reference documents in Annex A. Where further information is required, see Annex A for the references to the sources.

The recommendations given in this Technical Report are based on the *APEC Privacy Framework*, Directive 95/46/EC, Directive 2002/58/EC and the OECD Guidelines, instruments which cover most of the world.

NOTE While the OECD Guidelines and the *APEC Privacy Framework* are policy instruments which are advisory in nature, Directive 95/46/EC is mandatory for EU countries.

Most countries have pledged to use these instruments, along with specific national legislation, to implement basic principles of data privacy and protection of data held on individual persons. Although they vary in detail, the general principles are common and originate with the OECD Guidelines. Directive 95/46/EC is more specific, has more protection requirements and is mandatory for EU member states.

3.2 Privacy requires security

Privacy is required in ITS services and this involves following recognized and secure operations. Although this Technical Report does not specify such means, the following aspects should be considered (see references in Annex A).

Special attention should be given to the processing, transmission and storage of information, with authorized access for approved users and potential information flows with external entities which might get involved.

Moreover, in the ITS context, cooperation among the various organizations acquiring the information is often expected, in order to promote the exchange of data with the aim of improving functionalities in several ITS service domains. In this case, the comprehension of other particular requirements and interfaces which are often under undefined responsibilities also needs to be assessed in terms of security risks and possible threats to privacy.

Where appropriate, it is recommended that the guidelines defined for the management of information security in accordance with the ISO/IEC 27000 series of International Standards, with special reference to ISO/IEC 27002, be followed. The recommendations for the management of communications and operations or the measures taken in relation to the access control and privileges for authorized users should also be followed.

There are a number of security-related International Standards (including the ISO/IEC 27000 series) which can assist in the achievement of privacy (see Annex D).

3.3 The investigative process

Some examples are provided in this subclause to highlight data protection and data privacy aspects where existing law should be taken into consideration in the design of systems and standards. This Technical Report encourages an attitude of thinking similar to the specific recommendations implied by the *APEC Privacy Framework*, Directive 95/46/EC, Directive 2002/58/EC and the OECD Guidelines.

Firstly, certain significant technical scenarios were studied as examples in order to get an overview of the existing developmental situation. These are examples and do not purport to cover all ITS scenarios. Parallel to this, legal areas within public law, civil law and data privacy law are considered.

The results are quite interesting and important in terms of the legal implications, therefore, the most important results are briefly summarized for each scenario investigated.

For instance problems with data privacy laws might exist in many countries in terms of the installation of traffic monitoring cameras which can identify individual vehicle characteristics. In terms of civil law, it is advisable to clearly stipulate responsibilities concerning liability issues in regard to control units.

The issue of floating car systems is also relevant to basic fundamentals concerning the rights of the common person. It is the duty of the federal state to make sure that the rights of its citizens are not disproportionately limited. This problem, in regard to civil law, is also reflected in labour laws. The employer has to take the interests of his employees' protection into consideration. In some cases, the agreement of the workers' council is necessary.

Some parking schemes also raise concern because they save information related to mobile telephone numbers, license and registration numbers, bank accounts and names during the payment mode. It appears that the present payment methods are not in compliance with legal requirements for constitutional equality.

Regarding traffic monitoring in public areas, unequal treatment is to be avoided. For example cars that are equipped with monitoring chips should not be monitored more frequently than cars without chips.

Constitutional rights of freedom of movement are the most difficult in terms of legal data privacy considerations. For example within the European legislative framework, the Austrian investigation reached the opinion that road users have the constitutional right to travel freely in the public infrastructure network free from national monitoring. If monitoring is in the form of random sampling, the use of personal data can be justified if it increases safety in society, but only as long as no data is saved.

In terms of digital license plate numbers, the Austrian investigation concluded that privacy aspects need to be considered and specified in production specifications, and the specific terms of safety standards and liability determined in the case of injury and owed diligence, in particular between suppliers and system operators, and should be specified in terms of written contracts.

Another example involves the temporary opening of a motorway emergency lane and entrance controls on motorway ramps. When monitoring the emergency lane in all areas, issues about the data security of video cameras are important.

In the opinion of the Austrian investigation, the level of accepted prudence is potentially problematic in terms of civil law systems to reduce accident risks [e.g. intelligent speed adaptation (ISA), dynamic warnings, adaptive cruise control (ACC) and systems to avoid collisions].

Finally, questions are raised by the Austrian investigation concerning accident data loggers (UDS) and mayday systems. Two vehicles, one equipped with UDS and one without, should not be next to each other. UDS systems should save data in short intervals. Consideration for human dignity should also be made when using information from UDS systems.

On the one hand, this Technical Report demonstrates the “need to catch up” in the sense of legal aspects, but on the other hand, the Austrian study also highlights the legal inadmissibility of certain systems (at least within a European member state). Nevertheless, this Technical Report is designed to make the implementation of such systems possible and to help create legal clarity in the economic arena in order to achieve the necessary and important developments towards intelligent infrastructure.

The recommendations in this Technical Report are based on identified existing legal positions for each case, in order to ponder existing problems and to state needs for adaptation (*de lege lata*). A set of solutions (*de lege ferenda*) is discussed with the aim of reducing or eliminating these problems. The goal is to enable the implementation of these systems to the greatest extent possible; nevertheless the limits of these technical developments (constitutional and/or international law) should be shown and are shown. Furthermore, this Technical Report attempts to formulate basic principles from each aspect by establishing a (legally motivated) understanding of terms for intelligent infrastructure. Finally, based on these terms, the subjects are arranged based on their probable significance in legal order.

4 Recommendations

4.1 Basis of recommendations

This Technical Report proposes adherence to the following general principles for data protection and privacy of data relating to personal information concerning individuals.

The conditions under which data are collected and held in support or provision of ITS services should uphold all of the following principles.

4.2 Avoidance of harm

Data protection and privacy of data should recognize the interests of the individual to legitimate expectations of privacy, personal information protection and should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm can result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.

(*APEC Privacy Framework*, Part iii)

4.3 Fairly and lawfully

All personal data should be obtained and processed fairly and lawfully.

(*APEC Privacy Framework*, Part iii, I; Directive 95/46/EC, Chapter 3, Article 5; OECD Guidelines, Part 2, 7)

4.4 Specified, explicit and legitimate purposes

All personal data should be collected for specified, explicit and legitimate purposes.

[*APEC Privacy Framework*, Part ii (Cl.13); Part iii (Cl. 1)*;* Directive 95/46/EC, Section 2*,* Article 7, 7.14.1.1 Cl. 29, 30, 45, 51, 59; 7.19.5 (b); 7.19.7; OECD Guidelines, Cl. 7, 8]

4.5 Explicit and legitimate and must be determined at the time of collection of the data

The purposes for which personal data are collected should be determined at the time of the collection of the data, should be explicit and legitimate at the time of collection of the data and use of the data limited to the fulfilment of those purposes (or such others as are not incompatible with those purposes specified); the subsequent use should also be limited to the fulfilment of those purposes (or such others as are not incompatible with those purposes). All personal data collected should be adequate, relevant and not excessive in relation to the purposes for which they are processed.

[*APEC Privacy Framework*, 7.14.11 Cl. 28, 56,57; 7.19.5 (c); OECD Guidelines, Part 2. Cl. 9]

4.6 Not further processed in a way incompatible with the purposes for which they are originally collected

All personal data should not be further processed or used in a way incompatible with the purposes for which they are originally collected.

[Directive 95/46/EC, 7.14.1.1 Cl. 28, 29; 7.19.5 (b); 7.40.1 (2); OECD Guidelines, Part 1, Cl. 9, 24]

4.7 Not to be disclosed without the consent of the data subject

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with 4.4, except 4.7 a) or b):

a) where the data subject has freely and unambiguously given his/her consent;

b) by the authority of law of the country.

Processing of data is necessary:

— for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

— for compliance with a legal obligation to which the controller is subject;

— in order to protect the vital interests of the data subject;

— for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;

— 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 defined above.

[Directive 95/46/EC, Cl. 28, Cl. 30 and section D11, Cl. 7.19.13 2 d); OECD Guidelines, Part 1, Cl. 10; OECD Guidelines, Part 2, Cl. 9; *APEC Privacy Framework*, Part iv, Cl. 29]

4.8 Adequate, relevant and not excessive in relation to the purposes for which they are collected

All personal data should be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

[Directive 95/46/EC, Cl. 28, Cl. 30 and section D11, Cl7.19.13 2 d); OECD Guidelines, Part 1, Cl.10; OECD Guidelines, Part 2, Cl. 9; *APEC Privacy Framework*, Part iv, Cl. 29]

4.9 Accurate and, where necessary, kept up to date

All personal data should be accurate and, where necessary, kept up to date; every reasonable step should 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.

(*APEC Privacy Framework*, v1, Cl. 21; Directive 95/46/EC, section 1. 7.19.5; OECD Guidelines, Part 1, Cl. 8)

4.10 Identification of data subjects for no longer than is necessary for the purposes for which the data were collected

All personal data should be 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.

(*APEC Privacy Framework;* Directive 95/46/EC; OECD Guidelines)

4.11 Restriction to those who have a demonstrable “need to know”

Access to personal data should be restricted to the minimum number of persons who have a demonstrable “need to know”.

EXAMPLE In a situation where a law of the land has been allegedly infringed, an enforcement officer should have access only to information necessary to enforce and not all information pertaining to the individual subject, his ownership of vehicles or other personal data. That information can, for example only identify a vehicle and this data can be handed over to a prosecution system. A national prosecution service would, of course, require access to a great deal of information concerning the accused person in order to effect a prosecution, but all of this information should not be available to all enforcement officers and should not be made available without a justifiable need to know.

(OECD Guidelines, paragraph 1, 59)

The structure of systems and standards architecture for ITS should be constructed to enable the use of data to be restricted to those who have a genuine need to know.

4.12 Clear and accessible

Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information, which should include:

a) the fact that personal information is being collected;

b) the purposes for which personal information is being collected;

c) the types of persons or organizations to whom personal information might be disclosed;

d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information.

(*APEC Privacy Framework*, Part iii, Cl.15 and 20; Directive 95/46/EC, 7.9.1.2;)

4.13 Security safeguards

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

(*APEC Privacy Framework*, Part iii, vii, Cl. 22; OECD Guidelines, Part 2, Cl. 11)

4.14 Cumulative interpretation of multiple recommendations

In the development of ITS systems and standards, legislators and lawyers advise that the recommendations cannot just be taken individually, in isolation, but must also be viewed as a whole; this approach, which lawyers often refer to as “cumulative interpretation”, can lead to different interpretations, and this has significant implications. Examples are provided in Annex C.

Annex A
(informative)

Data privacy Framework, Directives and Guidelines

The references used for this Technical Report are the following:

a) *APEC Privacy Framework*, APEC#205-SO-01.2

http://www.dpmc.gov.au/privacy/apec/apec_privacy_framework.cfm or

http://epic.org/redirect/apf12407.html;

b) *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*

http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=31995L0046&model=guichett;

c) *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/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=32002L0058&model=guichett&lg=en;

d) *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*

http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

Annex B
(informative)

Example of national implementation of guidelines

B.1 Implementation of Directive 95/46/EC, Directive 2002/58/EC and the OECD Guidelines will vary according to the structure and practices of different regimes. As an example of the implementation of the *APEC Privacy Framework*, this annex shows some of the ways that a country (USA) is implementing it.

USNB Privacy Act provisions to make this Technical Report applicable to the USNB. The NIST Special Publication 800-12 Handbook provides guidelines for security planning and privacy protection within the security planning process.

B.1.1 The following are applicable US directives regarding privacy:

a) the Privacy Act of 1974;

b) the E-Government Act of 2002;

c) the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule;

d) Title 38 USC 5701;

e) Title 38 USC 5705;

f) Title 38 USC 7332;

g) the Freedom of Information Act of 1966;

h) the Computer Matching and Privacy Protection Act 1988;

i) the Gramm-Leach-Bliley Act of 1999;

j) the Clinger-Cohen Act of 1996;

k) the Paperwork Reduction Act of 1995;

l) the OMB Memo 06-15;

m) the OMB Memo 07-16;

n) the Children's Online Privacy Protection Act of 1998;

o) The Privacy Act of 1974, 5 USC § 552a, as amended;

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

http://crsc.nist.gov/publications/nistpubs/800-12/handbook.pdf

B.1.2 The following are the principles extracted from the OECD Guidelines and US DHEW:

a) lawful purpose: personal information should be collected only for lawful purposes;

b) relevance: information should be collected only if it is relevant for the purpose for which it is collected;

c) primary use: information should be used only for the purpose for which it was collected;

d) accuracy: only accurate information should be retained;

e) timeliness: information should be kept only for as long as it is timely;

f) completeness: incomplete information should not be kept, especially if the incompleteness is misleading;

g) access: data subjects should have access to information about themselves, and should be able to challenge and correct it;

h) security: information should be protected against unauthorized loss, alteration, or disclosure, both internal and external to the data collector; sensitive data requires greater protection;

i) transparency: the existence of a database containing personal information should not be secret;

j) accountability: enforcement mechanisms and effective oversight should be available to ensure compliance with these principles.

Annex C
(informative)

Examples of the principle of "cumulative interpretation"

As an example of the likely legal interpretations of Directive 95/46/EC, Directive 2002/58/EC and the *APEC Privacy Framework*, as well as the principle of "cumulative interpretation" (while recognizing that practices vary from country to country), if several articles of Directive 95/46/EC are compared, a "cumulative implication" on the use of data and the purposes for which it might be used can be seen. The example used in this annex is Directive 95/46/EC. However, the principle of "cumulative interpretation" described is just as applicable to the clauses of the *APEC Privacy Framework* or the OECD Guidelines (of course, Directive 95/46/EC has stronger legal requirement in Europe).

The preamble 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;

— 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 impact 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 solved in the courts. The objective of this Technical Report is to try to avoid these situations in the first place.

If a person gives 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 sentence: "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".

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 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 and WP29 have 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.

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. 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” (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 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 of vehicle manufacturers or vehicle registration databases of 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, paragraph 2 states: “Subject to adequate legal safeguards, **in particular that the data are not used for taking measures or decisions regarding any particular individua**l, 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." (highlighted in bold in this Technical Report).

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 extend privacy requirements for ITS systems and standards beyond the existing legal requirements or guidelines. However, it is advised 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 systems 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 systems 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 D
(informative)

Security-related International Standards

D.1 Generic security-related International Standards

There are a number of security-related ISO International Standards (including the ISO/IEC 27000 series), which may assist in the achievement of privacy, including:

ISO/IEC 17799, which establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 17799 contains best practices of control objectives and controls in the following areas of information security management:

— security policy;

— organization of information security;

— asset management;

— human resources security;

— physical and environmental security;

— communications and operations management;

— access control;

— information systems acquisition, development and maintenance;

— information security incident management;

— business continuity management;

— compliance.

The control objectives and controls in ISO/IEC 17799 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 17799 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices and helping to build confidence in inter-organizational activities.

ISO/IEC 18028 (all parts) defines techniques for securing inter-network connections that are established using virtual private networks (VPNs). It is relevant to all personnel who are involved in the detailed planning, design and implementation of VPN security (for example IT network managers, administrators, engineers, and IT network security officers).

The general objective of ISO/IEC 18028 (all parts) is to extend the security management guidelines provided in ISO/IEC 13335-1 and ISO/IEC 17799, by detailing the specific operations and mechanisms needed to implement network security controls in a wider range of network environments, providing a bridge between general IT security management issues and network security technical implementations.

ISO/IEC 18028-1 provides detailed guidance on the security aspects of the management, operation and use of IT networks and their interconnections.

ISO/IEC 18028-5 provides detailed guidance on the security aspects of the management, operation and use of IT networks and their interconnections. The objective of ISO/IEC 18028-5 is to provide support service to different organizations, IT network managers, administrators, technicians and IT security officers in choosing the appropriate VPN solution. It defines techniques for securing inter-network connections that are established using VPNs. It is relevant to all personnel who are involved in the detailed planning, design and implementation of VPN security (for example IT network managers, administrators, engineers and IT network security officers). ISO/IEC 18028-5 describes general principles of organization, structure, framework and usage of a VPN. It discusses functional areas, standards used and network protocols, the various types of VPNs and their respective requirements and characteristics.

ISO/IEC 27001 covers all types of organizations (e.g. commercial enterprises, government agencies and non-profit organizations). It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system (ISMS) within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. ISO/IEC 27001 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. It is intended to be suitable for the following:

a) use within organizations to formulate security requirements and objectives;

b) use within organizations as a way to ensure that security risks are cost effectively managed;

c) use within organizations to ensure compliance with laws and regulations;

d) use within organizations as a process framework for the implementation and management of controls to ensure that the specific security objectives of the organizations are met;

e) definition of new information security management processes;

f) identification and clarification of existing information security management processes;

g) use by the management of organizations to determine the status of information security management activities;

h) use by the internal and external auditors of organizations to determine the degree of compliance with the policies, directives and standards adopted by an organization;

i) use by organizations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with whom they interact for operational or commercial reasons;

j) implementation of business-enabling information security;

k) use by organizations to provide relevant information about information security to customers.

The technical content of ISO/IEC 27002 is identical to that of ISO/IEC 17799. ISO/IEC 27002 establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. It contains best practices of control objectives and controls in the following areas of information security management:

— security policy;

— organization of information security;

— asset management;

— human resources security;

— physical and environmental security;

— communications and operations management;

— access control;

— information systems acquisition, development and maintenance;

— information security incident management;

— business continuity management;

— compliance.

The control objectives and controls in ISO/IEC 27002 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 27002 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices and to help build confidence in inter-organizational activities.

ISO/IEC 27003[2)] — at the time of development of this Technical Report, this document is at Committee Draft status.

ISO/IEC 27004[3)] — at the time of development of this Technical Report, this document is at Committee Draft status.

ISO/IEC 27005 provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist in the satisfactory implementation of information security, based on a risk management approach. Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of ISO/IEC 27005. ISO/IEC 27005 is applicable to all types of organizations (e.g. commercial enterprises, government agencies and non-profit organizations), which intend to manage risks that could compromise the organization's information security.

ISO/IEC 27006 specifies requirements and provides guidance for bodies providing audit and certification of an ISMS, in addition to the requirements specified in ISO/IEC 17021 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification. The requirements contained in ISO/IEC 27006 need to be demonstrated in terms of competence and reliability by any body providing ISMS certification and the guidance given in ISO/IEC 27006 provides additional interpretation of these requirements for any body providing ISMS certification.

D.2 ITS-specific security International Standards

At the time of development of this Technical Report, there are several initiatives in progress, including the following.

ISO 24100 states the basic rules to be observed by service providers who handle personal data in probe vehicle information services. It is aimed at protecting personal data as well as the intrinsic rights and interests of probe data senders, i.e. owners and drivers of vehicles fitted with in-vehicle probe systems.

ISO 24100 specifies reference architecture for probe vehicle systems, a definition of personal data included in probe vehicle systems and the basic principles for personal data protection in probe vehicle systems.

Legislation and standards are being developed to support what is called “lawful intercept” and data retention for law enforcement, which adversely impact aspects of the privacy of personal data.

2) To be published.

3) To be published.

Bibliography

[1] ISO 24100, *Privacy — The basic principles for probe personal data protection*

[2] 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*

[3] ISO/IEC 17021, *Conformity assessment — Requirements for bodies providing audit and certification of management systems*

[4] ISO/IEC 17799, *Information technology — Security techniques — Code of practice for information security management*

[5] ISO/IEC 18028 (all parts), *Information technology — Security techniques — IT network security*

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

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

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

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

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

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

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

[13] *APEC Privacy Framework*, APEC#205-SO-01.2. Available from World Wide Web: http://www.apec.org

[14] *Convention for the Protection of Human Rights and Fundamental Freedoms*, Rome, 4.XI.1950. Available from World Wide Web: http://conventions.coe.int/treaty/EN/Treaties/html/005.htm

[15] *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Council of Europe, 28 January 1981. Available from World Wide Web: http://conventions.coe.int/Treaty/en/Treaties/Word/108.doc

[16] *Data Protection Act of Austria*, Austrian Data Protection Commission, Government of Austria

[17] *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*. Available from World Wide Web: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=31995L0046&model=guichett

[18] *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)*. Available from World Wide Web: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=32002L0058&model=guichett&lg=en

[19] NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*

[20] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Document C(80)58(Final), October 1, 1980

ICS 03.220.01; 35.240.60

Price based on 18 pages