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)

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 iv
Introduction v
1 Scope 1
2 Terms, definitions and abbreviated terms 1
2.1 Terms and definitions 1
2.2 Abbreviated terms 2
3 Background 2
3.1 Origin and basis of this Technical Report 2
3.2 Privacy requires security 3
3.3 The investigative process 3
4 Recommendations 5
4.1 Basis of recommendations 5
4.2 Avoidance of harm 5
4.3 Fairly and lawfully 5
4.4 Specified, explicit and legitimate purposes 5
4.5 Explicit and legitimate and must be determined at the time of collection of the data 5
4.6 Not further processed in a way incompatible with the purposes for which they are originally collected 5
4.7 Not to be disclosed without the consent of the data subject 6
4.8 Adequate, relevant and not excessive in relation to the purposes for which they are collected 6
4.9 Accurate and, where necessary, kept up to date 6
4.10 Identification of data subjects for no longer than is necessary for the purposes for which the data were collected 6
4.11 Restriction to those who have a demonstrable “need to know” 6
4.12 Clear and accessible 7
4.13 Security safeguards 7
4.14 Cumulative interpretation of multiple recommendations 7
Annex A (informative) Data privacy Framework, Directives and Guidelines 8
Annex B (informative) Example of national implementation of guidelines 9
Annex C (informative) Examples of the principle of “cumulative interpretation” 11
Annex D (informative) Security-related International Standards 14
Bibliography 17

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]