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.™

Document Sharing Hub

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 It supersedes PD ISO/TR 12859:2009 which is withdrawn.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.

© The British Standards Institution 2014. Published by BSI Standards Limited 2014

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

Documents
Document Sharing Hub

Full document details: PD CEN/TR 16742:2014

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

© 2014 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. CEN/TR 16742:2014 E

Documents
Document Sharing Hub

Full document details: PD CEN/TR 16742:2014

Contents

Page

Foreword 3

Introduction 4

1 Scope 5

2 Terms and definitions 5

3 Symbols and abbreviated terms 7

4 Background information 8
4.1 Historical background 8
4.2 Legal background 9
4.3 Fundamental Rights of Data Protection and Privacy 10

5 Basic elements of data protection and privacy 12
5.1 Personal information (PI) and its avoidance 12
5.1.1 General 12
5.1.2 GPS-Data or GPS-Trajectories 15
5.2 Sensitive data 16
5.3 Individual or data subject 16
5.4 Controller 17
5.4.1 General 17
5.4.2 ITS environment 17
5.5 Processor 18
5.6 Third Party 19
5.7 File or filing system (manually or automatically processed) 19
5.8 Consent 19
5.9 Withdrawal of consent 21
5.10 Fairness and legitimacy 21
5.11 Determination of purpose 21
5.12 Minimization of PI 22
5.13 Topicality and correctness of PI 22
5.14 Time limits to PI 23
5.15 Security requirements to PI 23
5.16 Obligation to keep PI secret 24
5.17 Obligation to inform the data subject (Individual or legal entity) 24
5.18 Right (access) to PI 25
5.19 Right to rectification and erasure of PI 26
5.20 Right to objection 27
5.21 Video surveillance (VS) 28
5.22 Shift in the burden of proof 28

Annex A (informative) Examples of the principle of “cumulative interpretation” 30

Annex B (informative) Data privacy Framework, Directives and Guidelines 33

Annex C (informative) Security related International Standards 34

Documents
Document Sharing Hub
Full document details: PD CEN/TR 16742:2014

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.

Documents
Document Sharing Hub
Full document details: PD CEN/TR 16742:2014

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)).

Documents
Document Sharing Hub
Full document details: PD CEN/TR 16742:2014

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

Documents
Document Sharing Hub
Full document details: PD CEN/TR 16742:2014

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]

Documents
Document Sharing Hub
Full document details: PD CEN/TR 16742:2014

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

Documents
Document Sharing Hub
Full document details: PD CEN/TR 16742:2014

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."

Documents
Document Sharing Hub
Full document details: PD CEN/TR 16742:2014

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);

Documents
Document Sharing Hub
Full document details: PD CEN/TR 16742:2014

— 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.

Documents
Document Sharing Hub
Full document details: PD CEN/TR 16742:2014