ISO/IEC JTC 1 N 9454

2008-12-16

ISO/IEC JTC 1
Information Technology

Document Type:	**Proposed NP**
Document Title:	**SC 36 New work item (NP) on "Information Technology – Identification of Privacy Protection Requirements pertaining to Learning, Education and Training (LET)"**
Document Source:	**SC 36 Secretariat**
Reference:	
Document Status:	**This document is circulated to JTC 1 National Bodies for concurrent review. If the JTC 1 Secretariat receives no objections to this proposal by the due date indicated, we will so inform the SC 36 Secretariat.**
Action ID:	**ACT**
Due Date:	**2009-03-16**
No. of Pages:	**27**

Secretariat, ISO/IEC JTC 1, American National Standards Institute, 25 West 43rd Street, New York, NY 10036; Telephone: 1 212 642 4932; Facsimile: 1 212 840 2298; Email: lrajchel@ansi.org

ISO/IEC JTC1 SC36 N1737

ISO/IEC JTC1 SC36
Information Technology for Learning, Education, and Training

Title:

New work item (NP) on "Information Technology – Identification of Privacy Protection Requirements pertaining to Learning, Education and Training (LET)"

Source:

JTC1/SC36 Ad-Hoc on Privacy

Project:

--

Document type:

Text for NP ballot

Status:

This document is circulated to SC36 P-members for ballot in accordance with Resolution 43 (Stuttgart 2008). The results will be discussed at the 2009-03 Wellington meeting.

Date:

2008-12-15

Action ID:

For ballot. Please use the electronic committee balloting application and vote **by 2009-03-15 at the latest.**

Distribution:

P, O, & L Members

ISO/IEC JTC1 SC36
Information Technology for Learning, Education, and Training

ISO/IEC JTC1/SC36
Document No: 36AHPN025

2008-12-03

Document Type:	Draft NWI
Document Title:	Draft text for NWIP "Information technology – Identification of Privacy Protection Requirements pertaining to Learning, Education and Training (LET)"
Document Source:	JTC1/SC36 Ad-Hoc on Privacy [Co-Rapporteurs: Peter Karlberg, Sylvie Arbouy and Jake Knoppers]
Project Number:	n/a
Document Status	-
Action ID:	For review and comment by JTC1/SC36 AHP participants no later than 12 December, 2008
Due Date:	2008-11-12
Distribution:	JTC1/SC36 AHP participants
No. of Pages:	27
Notes:	1. **Preparation of this Draft Text** At its Stuttgart, Germany September, 2008 Plenary Meetings, JTC1/SC36 adopted resolution #43 requesting its Ad-Hoc on Privacy (AHP to develop this NWI proposal (See JTC1/SC36 N1721. The SC36 AHP in turn decided to progress the development of this NWIP document based on its Stuttgart Meeting Report document 36AHP N024. The draft text which follows has been prepared by the three AHP Co-Rapporteurs, with the assistance of Renaud Fabre. 2. **Request for feedback and comment by 12 December, 2008** JTC1/SC36 AHP members, especially those who participated in the Stuttgart meetings are requested to provide comments, if they have any on the draft text for this NWIP document. Based on feedback received, the NWIP document will be finalized so that the NWI ballot document can be issued by 15 December, 2008. Responses to this request for comments should be forwarded Peter Karlberg (peter.karlberg@skolverket.se).

New Work Item Proposal

December 2008

PROPOSAL FOR A NEW WORK ITEM

Date of presentation of proposal: 2008-12-10	Proposer: JTC1/SC36 Ad-Hoc on Privacy
Secretariat: BSI	**ISO/IEC JTC 1 N** XXXX ISO/IEC JTC 1/SC 36 N xxxx 1737

A proposal for a new work item shall be submitted to the secretariat of the ISO/IEC joint technical committee concerned with a copy to the ISO Central Secretariat.

Presentation of the proposal

Title (subject to be covered and type of standard, e.g. terminology, method of test, performance requirements, etc.)

Information technology – Identification of Privacy Protection Requirements pertaining to Learning, Education and Training (LET)

Scope (and field of application)

This standard focuses on the identification of privacy protection requirements which apply to any JTC1/ SC36 LET standard:

- which involves the identification of an individual, (e.g., as a learner or student, a teacher, professor, or instructor, as an administrator, etc.), in the use and implementation of a JTC1/SC36 standard; and/or,
- which involves the recording and/or interchange of any information on or about an identifiable individual.

This standard identifies and summarizes principles governing privacy protection requirements which are generic in nature and applies them to the field of learning, education and/or training. This standard also incorporates best practices and policies as have already been implemented in LET environments in support of privacy protection requirements.

Exclusions

Excluded from the Scope of this standard are:

1) the specification of requirements of a functional services view (FSV) nature which include the development of mechanisms or information technologies pertaining to security techniques and services, communication protocols, etc. This includes existing standards (or standards under development of a FSV nature) which are already existing ISO/IEC JTC1, ISO, IEC and/or ITU standards. These include, but are not limited to, work relevant to privacy protection which is already covered by ISO/IEC JTC1 committees such as JTC1/SC17, JTC1/SC27, JTC1/SC32 or JTC1/SC37.

2) harmonization of overlap of and/or conflict of variances in privacy protection requirements among jurisdictional domains.

   While on the whole privacy or data protection requirements pertaining to the field of learning, education and/or training (LET) are similar in nature, i.e., at the primitive level, it is recognized that jurisdictional domains at various levels (especially in countries which have a federal form of government) may have variances in their privacy protection requirements.

Purpose and justification - attach a separate page as annex, if necessary

JTC1/SC36 adopted resolution #43 at its September, 2008 Stuttgart Plenary meeting requesting its Ad-Hoc on Privacy (AHP) to develop this NWI proposal. (see JTC1/SC36 N1721) This request for the development of this NWI was based on results of a (two year) Study Period by the JTC1/SC36 Ad-Hoc on Privacy which included a detailed survey of user requirements of its P-members as well as the identification and review of relevant standards and work of other ISO standards committees.

(See further Annex A)

Programme of work

If the proposed new work item is approved, which of the following document(s) is (are) expected to be developed?

___ a single International Standard
___ more than one International Standard (expected number: .....)
__x__ a multi-part International Standard consisting of ..... parts (See further Annex B)
____ an amendment or amendments to the following International Standard(s) .....
____ a technical report , type .....

And which standard development track is recommended for the approved new work item?

__X_a. Default Timeframe
____b. Accelerated Timeframe
____c. Extended Timeframe

Relevant documents to be considered

The document register of the SC36 Ad-Hoc on Privacy (AHP) serves as the source of the primary set of documents to be considered. (see www.jtc1sc36.org)

These SC36 AHP documents in turn identify many other documents including relevant international standards which will be considered in this standards project.

(For relevant documents, including standards, see further Annex C)

Co-operation and liaison

This standards development project will maximize cooperation and liaison with the already identified:

1) Committees of international standards bodies of the ISO, IEC, and ITU
   - JTC1/SC17
   - JTC1/SC27
   - JTC1/SC31
   - JTC1/SC32
   - JTC1/SC37
   - ISO COPOLCO
   - ISO TC68
   - ISO TC204
   - ISO TC215
   - ITU –T SG13
   - ITU-T JCA – Identity Management and Privacy

2) Non-international standards bodies
   - International Organization of Privacy and Data Protection Commissioners

(For more detailed information see further Annex D)

Will the service of a maintenance agency or registration authority be required? .....No.....
- If yes, have you identified a potential candidate? .....
- If yes, indicate name .....

Are there any known requirements for coding?.....No.....
-If yes, please specify on a separate page

Does the proposed standard concern known patented items?.....No.....
- If yes, please provide full information in an annex

Are there any known accessibility requirements and/or dependencies (see: http://www.jtc1access.org)? .....Yes.....(See E.2 below)
-If yes, please specify on a separate page

Are there any known requirements for cultural and linguistic adaptability? .....Yes.....
-If yes, please specify on a separate page (See E.1 below)

Comments and recommendations of the JTC 1 or SC 36 Secretariat - attach a separate page as an annex, if necessary

Comments with respect to the proposal in general, and recommendations thereon:
It is proposed to assign this new item to JTC 1/SC 36/WG3-Participant Information

Voting on the proposal - Each P-member of the ISO/IEC joint technical committee has an obligation to vote within the time limits laid down (normally three months after the date of circulation).

Date of circulation:	**Closing date for voting:**	**Signature of Secretary:**
2008-12-15	2009-03-15	D Hyde

NEW WORK ITEM PROPOSAL - PROJECT ACCEPTANCE CRITERIA		
Criterion	**Validity**	**Explanation**
A Business Requirement		
A.1 Market Requirement	Essential __X_ Desirable ___ Supportive ___	There is a growing concern on privacy protection issues in the field of learning, education and training (LET). Ensuring that privacy protection requirements mentioned in this work item are essential to many ITLET applications. See results of JTC1/SC36 Survey of its P-members on the need for standards development in support of privacy/data protection requirements applicable to learning, education and training (LET). JTC1/SC36 Survey document is JTC1/SC36 N1436. The P-members responses to this Survey, as well as other contribution from P-members, the resolution of the JTC1/SC36 Ad-Hoc on Privacy, and related documents are posted as publicly available documents on the JTC1/SC36 sub-folder for its Ad-Hoc on Privacy.

NEW WORK ITEM PROPOSAL - PROJECT ACCEPTANCE CRITERIA		
A.2 Regulatory Context	Essential __X_ Desirable ___ Supportive ___ Not Relevant ___	See results of JTC1/SC36 Survey of its P-members on the need for standards development in support of privacy/data protection requirements applicable to learning, education and training (LET). JTC1/SC36 Survey document is JTC1/SC36 N1436. The P-members responses to this Survey, as well as other contribution from P-members, the resolution of the JTC1/SC36 Ad-Hoc on Privacy, and related documents are posted as publicly available documents on the JTC1/SC36 sub-folder for its Ad-Hoc on Privacy. NOTE 1: Privacy protection requirements do not apply to JTC1/SC36 e-learning standards where these, 1) do not involve or require the recording of information on or about an identifiable individual; 2) pertain to personal information which is often in the public domain, (e.g., as an author of a learning resource); and/or, NOTE 2: where the “human being” acts in the role of “organization Person”, (e.g., certain personal information elements are public for natural persons in their role as a member of a faculty of a university, college, school, etc., or as an employee of a public administration, an organization (of any type), etc.).
B. Related Work		
B.1 Completion/Maintenance of current standards	Yes ___ No___x	
B.2 Commitment to other organization(s)	Yes __x_ No___	See above under “Cooperation and Liaison” as well as in Annex D
B.3 Other Source of standards	Yes __x_ No___	Many standards which will serve as sources for the development of this work item have been identified. (See further Annex C)
C. Technical Status		
C.1 Mature Technology	Yes __x_ No___	Most of the requirements are well-known. They need to be captured and specified from a JTC1/ SC36 LET perspective
C.2 Prospective Technology	Yes ___ No__x_	This standards project will be IT-platform neutral and is intended to be able to be implemented on any existing or prospective IT-technology platform.
C.3 Models/Tools	Yes ___x No___	This standards project supports an IT-enabled approach including its models and tools being rule-based thereby facilitating the implementation on a variety of IT-platforms
D. Conformity Assessment and Interoperability		
D.1 Conformity Assessment	Yes ___ No__X_	Criteria will be determined but this standard will not provide conformance tests

NEW WORK ITEM PROPOSAL - PROJECT ACCEPTANCE CRITERIA		
D.2 Interoperability	Yes _x__ No___	This standard project maximizes the capture and specification of common legal and operational requirements, thereby maximizing interoperability in the interchange of personal information in LET applications
E. Cultural and Linguistic Adaptability		
E.1 Cultural and Linguistic Adaptability	Yes – X – No _____	This standard will be architected and structured to be able to support cultural and linguistic adaptability requirements (in general) and in particular those which form part of privacy protection requirements. Here there will be close cooperation with JTC1/ SC36/WG7 which develops standards in this field.
E.2 Adaptability to Human Functioning and Use	Yes – X – No _____	Individual accessibility requirements (e.g. Access for All-AfA) will be recognized and supported in the development of this standards work. This will be done in close cooperation with SC36/WG7 whose work programme includes the multipart ISO/IEC 24751 Individual Accessibility. Standards project (of which the first three Parts are already an IS).
F. Other Justification		

Notes to Proforma

A. Business Relevance. That which identifies market place relevance in terms of what problem is being solved and or need being addressed.

A.1 Market Requirement. When submitting a NP, the proposer shall identify the nature of the Market Requirement, assessing the extent to which it is essential, desirable or merely supportive of some other project.

A.2 Technical Regulation. If a Regulatory requirement is deemed to exist - e.g. for an area of public concern e.g. Information Security, Data protection, potentially leading to regulatory/public interest action based on the use of this voluntary international standard - the proposer shall identify this here.

B. Related Work. Aspects of the relationship of this NP to other areas of standardisation work shall be identified in this section.

B.1 Competition/Maintenance. If this NP is concerned with completing or maintaining existing standards, those concerned shall be identified here.

B.2 External Commitment. Groups, bodies, or fora external to JTC 1 to which a commitment has been made by JTC for Co-operation and or collaboration on this NP shall be identified here.

B.3 External Std/Specification. If other activities creating standards or specifications in this topic area are known to exist or be planned, and which might be available to JTC 1 as PAS, they shall be identified here.

C. Technical Status. The proposer shall indicate here an assessment of the extent to which the proposed standard is supported by current technology.

C.1 Mature Technology. Indicate here the extent to which the technology is reasonably stable and ripe for standardisation.

C.2 Prospective Technology. If the NP is anticipatory in nature based on expected or forecasted need, this shall be indicated here.

C.3 Models/Tools. If the NP relates to the creation of supportive reference models or tools, this shall be indicated here.

D. Conformity Assessment and Interoperability Any other aspects of background information justifying this NP shall be indicated here.

D.1 Indicate here if Conformity Assessment is relevant to your project. If so, indicate how it is addressed in your project plan.

D.2 Indicate here if Interoperability is relevant to your project. If so, indicate how it is addressed in your project plan

E. **Cultural and Linguistic Adaptability** Indicate here if cultural and linguistic adaptability is applicable to your project. If so, indicate how it is addressed in your project plan.

F. Other Justification Any other aspects of background information justifying this NP shall be indicated here

Annex A – Purpose and Justification

JTC1/SC36 considers it important that international standards which facilitate the use of information and communication technologies (ICT) be structured to be able to support legal requirements of the jurisdictional domains in which they are to be implemented and used. This is particularly so where such standards are used to capture and manage recorded information used in decision-making about individuals. Common legal and regulatory requirements of this nature, which impact the development of ICT-based standards, include those of a public policy nature such as those pertaining to consumer protection, privacy protection, individual accessibility[1], human rights, etc.

The role of ISO/IEC JTC1/SC36 is to develop ICT-based standards in the fields of learning, education and training (LET). Since the application and use of a majority of JTC1/SC36 standards involve the role of an individual as "learner", this means that any recorded information on or about an identifiable individual as a "learner" is subject to applicable privacy/data protection requirements.

Within the international standards organizations of the ISO, IEC, and ITU, various standards development committees are addressing the issue of privacy/data protection in their particular areas of responsibility[2]. Consequently, many standards development projects addressing privacy/data protection requirements in a specified area of application are under way, near completion, or in process of being launched.[3]

Given the importance of ensuring that its standards development projects also support privacy/ data protection requirements, where applicable, JTC1/SC36 decided at its 2006 Wuhan China Plenary meeting, to establish an "Ad-Hoc Group on Privacy (AHP). A key work component of this Ad-Hoc Group on Privacy was to undertake a survey on privacy requirements of its P-member bodies in the field of information technology for learning, education and training (ITLET).

(The mandate and objectives of this JTC1/SC36 AHP as well as the Survey instrument are stated in document 36N1436).

The results of the work of the JTC1/SC36 Ad-Hoc on Privacy, including that of its "Questionnaire" as a key instrument in its Survey on Privacy Protection requirements for education, learning and training (LET)", demonstrated clearly the need for this proposed standards project[4]. Additional contributions to the AHP provided further documentation on the need for this standards project.

In addition, the vast majority of JTC1/SC36 P-members represent jurisdictional domains which are governed by privacy/data protection requirements of a legislative/regulatory nature.

---

[1] ISO/IEC JTC1/SC36 has developed a multipart international standard in support of "individual accessibility" requirements including those of a legal and/or regulatory nature. Of this multipart standard, the first three parts are completed having reached the final (FDIS) stage. The title of this multipart standard and its first three parts are: *ISO/IEC 24751 "Individual Adaptability and Accessibility in e-Learning, Education and Training".*

- Part 1: Framework and Reference Model;
- Part 2: "Access For All" Personal Needs and Preferences for Digital Delivery;
- Part 3: "Access for All" Digital Resource Description.

[2] Examples here include ISO, IEC, ISO/IEC JTC1, and ITU committees in banking/financial services, e-business, transportation, health/medical, identification cards, automated data capture, biometrics, security, data management and interchange, telecommunication services, etc.

[3] These privacy/data protection related standards development projects have already been identified by the JTC1/SC36 Ad-Hoc on Privacy. See also below Annex C.

[4] The predominant set of respondents here were "Ministries of Education" whose requirements were consolidated in the JTC1/SC36 P-member responses.

Consequently, for any JTC1/SC36 standard which pertains to “individuals” as participants in a learning process, to be able to be implemented and used in the jurisdictional domain of the P-members, it must be able, or structured to be able, to support applicable privacy protection requirements.

Annex B - Programme of Work – Option of a single or multipart standard[5]

In making a proposal for a new standard development project, one has the option of either addressing all the issues to be addressed in a "single" standard or in a "multipart" standard.

Given the responses of SC36 P-members to the original SC36N1436 "Privacy Survey" as well as the discussions of the SC36 Ad-Hoc on Privacy (AHP) meetings, particularly the most recent one in Stuttgart, Germany, September, 2008, the SC36 AHP decided to take the approach of a "multipart" standards project. The reasons for such an approach include:

- the need and ability to be able to differentiate between common, generic privacy protection principles for LET on the one hand, and the other, those issues which are specific or particular in nature, (e.g., as already identified by JTC1/SC36 P-members in their responses to the "Privacy Survey" and other contributions to the work of the SC36 AHP);

- the need to prioritize on (1) identification and synthesis of the operational view requirements, (e.g., user requirements, generic privacy protection legal/regulatory requirements, current best practices and policies), i.e., the "WHATs" versus, (2) the functional support services and related technical related mechanisms from an ICT support infrastructure perspective, i.e., as the possible various "HOWs".

Trying to address both the "WHATs" and "HOWs" in a single standard (document), all theSC36 P-member requirements identified as a result of the SC36 AHP, will most likely result in a standard development project which will be very difficult to integrate, take a very long time, and does not have a goal probability of success.

In addition, there is an urgent need to having a base or "Framework" standard developed and completed as quickly as possible due to the urgent needs of prospective users.

Taking a "multipart" standard approach here has many benefits including:

1) being able to have a "short" Part 1 "Framework" (which states the key principles for privacy protection as applicable to e-learning, key concepts and their definitions, and the rules governing the development of additional Parts)[6];

2) having the flexibility for JTC1/SC36 P-members to be able to decide which of the privacy protection issues already identified [7]as part of the Privacy Survey need to be combined in one focused Part and which in another Part;

3) having the flexibility to decide whether or not a new Part 2+ should be of the nature of an "IS" (= international standard) or "TR" (= Technical Report);

---

5 See also below Annex E "*Identification pf specific "sub-times" of work and their priorities*".

6 Such a Part 1 should include the informative Annex listing all the laws, regulations, policies, etc., of a privacy protection nature which apply. These would include those already provided by SC36 P-members in response to the eLearning and privacy protection survey, i.e., in response to 36N1436 as well as those provided in the course of the development of Part 1 of the multipart standard. For a successful example of the application of such an approach, see *Annex C (Informative) Accessibility policies and legislation/ Politiques et legislation en matières d'accessibilité in Individualized Adaptability and Accessibility in e-Learning, Education and Training – Part 1: Framework and Reference Model / Adaptabilité et accessibilité en e-apprentissage, éducation et formation - Partie 1: Cadre et modèle de référence*

7 See further below Annex E "*Identification of specific "sub-items" of work and their priorities".*

4) being able to have a specific part deal with various functional services, i.e., technology dependent matters, and providing linkages/bindings to specific IT-platforms and/or information technologies;

5) being able to keep both the Part 1 Framework Model and the Parts 2+ “short” and very focused ;

6) being able to progress the development of several Parts in parallel.

Annex C - Relevant Documents to be considered

Relevant document to be considered are presented below in two categories, namely,

- C.1 ISO standards (including those under development) of relevance as identified by the JTC1/SC36 Ad-Hoc on Privacy as well as searches of the ISO database on standards; and,
- C.2 Other documents identified by JTC1/SC36 Ad-Hoc on Privacy.

C.1 ISO standards (including those under development) of relevance as identified by the JTC1/ SC36 Ad-Hoc on Privacy as well as searches of the ISO database on standards

C.1.1 Introductory Notes

1.1.1 Annex C contains a preliminary list of existing ISO/IEC or ISO standards (as well as those under development) whose title or scope statement indicates that they may pertain to or contain elements pertaining to privacy/data protection requirements.

This list is part of the development work by the JTC1/SC36 Ad-Hoc on Privacy. It is based on the principle of maximizing use of existing ISO standards in this new standards development work by JTC1/SC36.

1..1.2 This preliminary list below is based on searches of the "iso.org" database of existing or under development standards which were identified using searches on the ISO standards database with as keywords "individual", "personal information", "privacy", and " data protection".

However, the "iso.org" search engine supports only a very primitive level of search capabilities. It appears that Boolean type searches are not supported, (e.g., even the use of the simple "AND" operator to focus a search and reduce the number of hits is not supported). It appears that one is permitted to use on one "search term"[8].

The results of these "primitive searches" are as follows:

Search Term	**No. of "Relevant Standards Identified by "iso.org" website based on a "full search"**
privacy	204
data protection	484
personal information	491

1.1.3 With respect to the list of existing (or under development) ISO standards the following assumptions are made with respect to the development of this NWI.

(1) many of the requirements as specified in existing ISO standards pertaining to ensuring the trustworthiness, integrity, timeliness, accuracy, relevancy of the recorded information about an identified entity are not unique to privacy protection requirements in the filed of learning, education and training.

Based on a preliminary review of a number of the existing ISO standards identified below, it is most likely that 75% of the normative elements of this new

---

[8] An "advanced" or "extended" search based on Boolean logic here would be as follows (with "personal information", "data protection", "personal information" not being considered a compound term)

- (privacy) OR (data AND protection) OR (personal AND information) OR (personal AND identification) AND (individual)

If the terms "data protection", "personal information" ; personal information are considered as compound terms, the search strategy would be:

- (privacy OR data protection OR personal information) OR personal information) AND individual.

JTC1/SC36 standard will be based on normative elements of existing ISO standards.

(2) one cannot assume that the ISO standards listed below represent a "harmonized" approach. As such, the development of JTC1/SC36 ITLET Privacy protection standard. will ensure an integrated and harmonized approach to the development of privacy protection requirements for LET..

(3) a substantial number of "consumer protection" requirements are very similar (if not the same) as "privacy protection" requirements. Consequently, ISO standards identified below of a consumer protection nature (for which the ISO committee responsible is "COPOLCO") are of particular relevance;

(4) many ISO standards existent which pertain to and support generic data protection requirements with respect to recorded information in an IT-system Also many of these are IT-neutral in nature and pertain to any set of recorded information (SRI) irrespective of, and independent whether such an "SRI" pertains to personal information, i.e., that on or about an identifiable individual.

(5) many ISO standards exist which pertain to and support generic information management, data management and interchange requirements applicable to to any set of recorded information (SRI) irrespective of whether or not it pertains to an "identifiable individual", i.e., is "personal information";; and,

(6) the development of this new standard will also takes into account the fact that in order to meet "individual accessibility' requirements[9] of an "individual" as a user, it is necessary to be able to support individual user needs and preferences in their use of ICTs based applications.

C.1.2 Organization of Listing in Matrix Form

A matrix form is used as follows:

Col. No.	Col. Title	Use
1	ISO ID	ISO ID for the standard
2	ISO Responsible Committee	ISO committee responsible for the standard
3	Title	Title of the standard

ISO ID	ISO Responsible Committee	Title
(1)	(2)	(3)
IWA 2:2007	TMB	Quality management systems – Guidelines for the application of ISO 9001:2000 in education
ISO/IEC Guide 14:2003	COPOLCO	Purchase information on goods and services intended for consumers
ISO/IEC Guide 71:2001	TMB	Guidelines for standards developers to address the needs of older persons and persons with disabilities
ISO/IEC 2382-1:1993	JTC1	Information technology – Vocabulary – Part1: Fundamental terms
ISO/IEC 2382-8:1998	JTC1	Information technology – Vocabulary – Part 8: Security

[9] Increasingly within many jurisdictional domains including most of the ISO/IEC JTC1 members) as well as at the UN level, there are now legal requirements for and any all ICT implementation to be able to ensure that "disabled" individuals are ensure equal access to the use of ICT, especially those involving WWW/Internet-based access. As this requires the ability to be able to support personal preferences its requires the individual to specify and provide "personal information".

ISO ID	ISO Responsible Committee	Title
ISO 5127:2001	TC46	Information and documentation – Vocabulary
ISO/IEC 7501-1:2005	JTC1/SC17	Identification cards - Machine readable travel documents – Part 1: Machine readable passport (5th ed.)
ISO/IEC 7812-1:2006	JTC1/SC17	Identification cards – Identification of issuers – Part 1: Numbering system
ISO/IEC 7812-2:2007	JTC1/SC17	Identification cards – Identification of issuers – Part 2: Application and registration procedures
ISO/IEC 7813:2006	JTC1/SC17	Information technology – Identification cards – Financial transaction cards
ISO/IEC 7816-11:2004	JTC1/SC17	Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods
ISO/IEC 7816-13:2007	JTC1/SC17	Identification cards – Integrated circuit cards – Part 13: Commands for application management in a multi-application environment
ISO 8459-4:1998	TC46/SC4	Information and documentation – Bibliographic data element directory – Part 4: Circulation application
ISO 8459-5:2002	TC46/SC4	Information and documentation – Bibliographic data element directory – Part 5: Data elements for the exchange of cataloguing and metadata
ISO 9127:1988	JTC1/SC7	Information processing systems – User documentation and cover information for consumer software packages
ISO 9564-1:2002	TC68/SC2	Banking – Personal Information Number (PIN) management and security – Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems
ISO/IEC 9594-1:2001	JTC1/SC6	Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services
ISO 9737-7:2002	TC154	Electronic data interchange for administration, commerce and transport (EDIFACT) – Application level syntax rules (Syntax version number:4, Syntax release number: 1) Part 7: Security rules for batch EDI (confidentiality)
ISO/IEC TR 9789:1994	JTC1/SC32	Information technology – Guidelines for the organization and representation of data elements for data interchange – Coding methods and principles
ISO/IEC 9798-1:1997	JTC1/SC27	Information technology – Security techniques- Entity authentication – Part1: General
ISO/IEC TR 10032:2003	JTC1/SC22	Information technology – Reference model of data management
ISO 9999:2007	TC173/SC2	Assistive products for persons with disability – Classification and terminology
ISO/IEC 10181-1:1996	JTC1	Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 1: Overview
ISO/IEC 10181-2:1996	JTC1	Information technology – Open Systems Interconnection – Security frameworks for open systems- Part 2: Authentication framework
ISO/IEC 10181-4:1997	JTC1	Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework
ISO/IEC 10181-5:1996	JTC1	Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework
ISO 11568-1:2005	TC68/SC2	Banking – Key management (retail) – Part 1: Principles
ISO/IEC 11770-1:1996	JTC1/SC27	Information technology – Security techniques – Key management – Part 1: Framework

ISO ID	ISO Responsible Committee	Title
ISO TR 13569:2005	TC68/SC2	Financial services – Information security guidelines
ISO/DIS 13606-1	TC215	Health informatics – Electronic health record communication – Part 1: Reference model
ISO 14155-1:2003	TC194	Clinical investigation of medical devices for human subjects – Part 1: General requirements
ISO/IEC 14662:2006	JTC1/SC32	Open-edi reference model
ISO TS 14904:2002	ISO TC 204	Road transport and traffic telematics – Electronic fee collection (EFC)-Interface specification for clearing between operators
ISO 15489-1:2001	TC46/SC11	Information and documentation – Records management – Part 1: General
ISO/TR 15489-2:2001	TC46/SC11	Information and documentation – Records management – Part 2: Guidelines
ISO/TR 15766:2000	TC22/SC12	Information technology – Security techniques – Security information objects for access control
ISO/IEC 15816:2002	JTC1/SC27	Information technology – Security techniques – Security information objects for access control
ISO/IEC 15944-1: 2002	JTC1/SC32	Informative technology – Business Operational View - Part 1: Operational Aspect of Open-edi for implementation
ISO/IEC 15944-2:2006	JTC1/SC32	Informative technology – Business Operational View – Part 2: Registration of scenarios and their components as business objects
ISO/IEC 15944-2:2007	JTC1/SC32	Informative technology – Business Operational View - Part 4: Business transaction scenarios – Accounting and economic ontology
ISO/IEC 15944-2:2008	JTC1/SC32	Informative technology – Business Operational View: - Part 5: Identification and referencing of requirements of jurisdictional domains as sources of external constraints
ISO/IEC 15944-2:2008	JTC1/SC32	Informative technology – Business Operational View- Part 6: Technical aspects of eBusiness Modelling
ISO/IEC FDIS 15944-2:2008	JTC1/SC32	Informative technology – Business Operational View – Part 7: eBusiness Vocabulary
ISO/IEC CD 15944-2:2008	JTC1/SC32	Informative technology – Business Operational View – Part 8: Identification of privacy protection requirements as external constraints on business transaction
ISO/TR 16056-1:2004	TC215	Health informatics – Interoperability of telehealth systems and networks – Part 1: Introduction and definitions
ISO/TS 16058:2004	TC215	Health informatics – Interoperability of telelearning systems
ISO/PAS 17002:2004	CASCO	Conformity assessment – Confidentiality – Principles and requirements
ISO/PAS 17004:2005	CASCO	Conformity assessment – Disclosure of information – Principles and requirements
ISO/TS 17090-1:2002	TC215	Health informatics – Public key infrastructure – Part 1: Framework and overview
ISO/TR 17119:2005	TC215	Health informatics – Health informatics profiling framework
ISO/TS 17573:2003	TC204	Road Transport and Traffic Telematics – Electronic Fee Collection (EFC) – Systems architecture for vehicle related transport services
ISO/TS 17574:2004	TC204	Road transport and traffic telematics – Electronic fee collection (EFC) – Guidelines for EFC security protection profiles

ISO ID	ISO Responsible Committee	Title
ISO/IEC 18013-1:2005	JTC1/SC17	Information technology – Personal identification – ISO-compliant driving licence – Part 1: Physical characteristics and basic data set
ISO/IEC FCD 18013-2	JTC1/SC17	Information technology – Personal identification – ISO-compliant driving licence – Part 2: Machine readable technologies
ISO/IEC 18014-1:2002	JTC1/SC27	Information technology – Security techniques – Time stamping services – Part 1: Framework
ISO 18185-4:2007	TC104/SC4	Freight containers – Electronic seals – Part 4: Data protection
ISO/TR 18307:2001	TC215	Health informatics – Interoperability and compatibility in messaging and communication standards – Key characteristics
ISO/TS 18308:2004	TC215	Health informatics – Requirements for an electronic health record architecture
ISO 19092-1:2006	TC68/SC2	Financial services – Biometrics – Part 1: Security framework
ISO/IEC 19794-1:2006	JTC1/SC37	Information technology – Biometric data interchange formats – Part 1: Framework
ISO/IEC TR 19765:2007	JTC1/SC35	Information technology – Survey of icons and symbols that provide access to functions and facilities to improve the use of information technology products by the elderly and persons with disabilities
ISO/IEC TR 19766:2007	JTC1/SC35	Information technology – Guidelines for the design of icons and symbols accessible to all users, including the elderly and persons with disabilities
ISO 20252:2006	TC225	Market, opinion and social research – Vocabulary and service requirements
ISO 20302:2006	TC215	Health informatics – Health cards – Numbering system and registration procedure for issuer identifiers
ISO 23081-1:2006	TC46/SC11	Information and documentation – Records management processes – Metadata for records – Part 1: Principles
ISO/TR 20514:2005	TC215	Health informatics – Electronic health record – Definition, scope and context
ISO/IEC 21000-4:2006	JTC1/SC29	Information technology – Multimedia framework (MPEG-21) – Part 4: Intellectual Property Management and Protection Components
ISO/TR 21089:2004	TC215	Health informatics – Trusted end-to-end information flows
ISO/TS 21091:2005	TC215	Health informatics – Directory services for security, communications and identification of professionals and patients
ISO 21549-2:2004	TC215	Health informatics – Patient healthcard data – Part 2: Common objects
ISO 21549-3:2004	TC215	Health informatics – Patient healthcard data – Part 3: Limited clinical data
ISO 21549-4:2006	TC215	Health informatics – Patient healthcard data – Part 4: Extended clinical data
ISO 21549-7:2007	TC215	Health informatics – Patient healthcard data – Part 7: Medication data
ISO/TR 22221:2006	TC215	Health informatics – Good principles and practices for a clinical data warehouse
ISO/DIS 22307	TC68/SC7	Financial services industry – Privacy impact assessment
ISO/TS 22600-1:2006	TC215	Health informatics – Privilege management and access control – Part 1: Overview and policy management
ISO/TS 225600-2:2006	TC215	Health informatics – Privilege management and access control – Part 2: Formal models

ISO ID	ISO Responsible Committee	Title
ISO 22857:2004	TC215	Health informatics – Guidelines on data protection to facilitate trans-border flows of personal health information
ISO/CD 24100	TC204	Privacy – the basic principles for probe personal data protection
ISO/IEC 24703:2004	JTC1/SC36	Information technology – Participant Identifiers
ISO/IEC CD TR 24714-1	JTC1/SC37	Cross-jurisdictional and societal aspects of implementation of biometric technologies – Part 1: Guide to the accessibility, privacy and health and safety issues in the deployment of biometric sys5tems for commercial application
ISO/IEC 24751-2:2008	JTC1/SC36	Information technology – Individualized adaptability and accessibility in e-learning and training – Part 2: "Access for all" personal needs and preferences for digital delivery
ISO/IEC WD 24751-5	JTC1/SC36	Information technology – Individualized adaptability and accessibility in e-learning, education and training – Part 5: Personal needs and preferences for non-digital resources
ISO/IEC WD 24751-6	JTC1/SC36	Information technology – Individualized adaptability and accessibility in e-learning, education and training – Part 6: Personal needs and preferences for description of events and places
ISO/IEC CD 24571-8:2008	JTC1/SC36	Information technology – Individualized adaptability and accessibility in e-learning, education and training – Part 8: Language accessibility and HIEs in e-Learning applications: Principles, rules and metadata elements
ISO/IEC 27002:2005	JTC1/SC27	Information techniques – Code of practice for information security management
ISO/DIS 27799	TC215	Health informatics – Information security management in health using ISO/IEC 17799
ISO/DIS 28000	TC8	Specification for security management systems for the supply chain
ISO/DIS 28001	TC8/SC11	Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance

1) The Referenced Specifications to be included in the CD document for this NWI will be:
   - taken from those already serving as Referenced Specifications for one or more Parts of ISO/IEC 15944; and,
   - those which need to be added such as:
     (a) the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data;
     (b) Directive 95/46/EC of the European Parliament and the Council of 24 October, 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data;
     (c) The UN Convention of the Rights of Persons with Disabilities

C.2 Other documents identified by JTC1/SC36 Ad-Hoc on Privacy

- SC27 WD 29100 A Privacy framework

- SC27 WD 29115 Authentication assurance

- SC27 WD 24760 A framework for identity management
- SC27 WD 29101 A Privacy Reference Architecture
- SC27 WD 29146 A framework for access management
- SC37 - NWI Information technology – Automatic identification and data capture techniques – Mobile item identification and management – Consumer privacy-protection protocol for Mobile RFID services
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines)
- OECD Policy Guidance on Radio Frequency Identification
- CWA DPP European Best Practices (draft)
- CWA DPP Audit tools for manager (draft)
- CWA DPP Voluntary Technology Dialogue System (draft)
- CWA 15262:2005 Inventory of Data Protection Auditing Practices
- CWA 15263:2005 Analysis of Privacy Protection Technologies, Privacy- Enhancing Technologies (PET), Privacy Management Systems (PMS) and Identity Management systems (IMS), the Drivers thereof and the need for Standardization
- CWA 15292:2005 Standard form contract to assist compliance with obligations imposed by article 17 of the Data Protection Directive 95/46/EC (and implementation guide)
- CWA 15499-01:2006 Personal Data Protection Audit Framework (EU Directive EC 95/46) Part I: Baseline Framework - The protection of Personal Data in the EU
- CWA 15499-02:2006 Personal Data Protection Audit Framework (EU Directive EC 95/46), Part II: Checklists, questionnaires and templates for users of theframework - The protection of Personal Data in the EU
- CWA (draft) Unique identity systems for organisations and parts thereof (CEN WS Cyber Id.)
- Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the field of Information and Communication Technologies, applied to Radio Frequency Identification (RFID) and systems (§ privacy and data protection)

Annex D Co-Operation and Liaison

Cooperation and liaison are presented below in two categories, namely,

- D.1 ISO/IEC, ISO, ISO and ITU Committees
- D.2 Other committees and organizations of interest

D.1 ISO/IEC, ISO, ISO and ITU Committees[10]

- JTC1/SC17 – Cards and personal identification
  - WG 3 Identification cards – Machine readable travel document
  - WG 10 – Motor vehicle driver licenses and related documents
  - WG 11 – Application of biometrics to cards and personal identification
- JTC1/SC27 – IT Security techniques
  - WG 5 – Identity management and privacy technologies
- JTC1/SC31 – Automatic identification and data capture techniques
- JTC1/SC32 – Data management and interchange
  - WG1 eBusiness
- JTC1/SC37 – Biometrics
  - WG 6 Cross-Jurisdictional and Societal Aspects of Biometrics
- ISO CASCO - Committee on Conformity Assessment
- ISO COPOLCO -Committee on Consumer Policy
- ISO TC68 – Financial services
  - SC7/WG5 –Privacy impacts assessment standard
- ISO TC204 – Intelligent transportation systems
- ISO TC215 – Health informatics
  - WG4 – Security
  - WG 5- Health cards
- ITU –T SG13 /17 – IdM Identity Management and Privacy
- ITU-T JCA – IdM Identity Management and Privacy
- ITU-T WP 2/17 Biometrics

D.2 Other committees and organizations of interest

- International Conference of Privacy and Data Protection Commissioners
- OECD - Working Party on Information Security and *Privacy* (WPISP)
- European Commission – Article 29 Data protection working party
- EU "7 Framework programme "– Senior- Social, ethical and privacy needs in ICT for older people
- CEN ISSS WS DPP Data Protection & Privacy
- CEN ISSS WS Cyber Identity
- PICOS Biometrics, Identity Management and Privacy
- PrimeLife Biometrics, Identity Management and Privacy
- FIDIS Biometrics, Identity Management, and Privacy
- Liberty Alliance Identity Management

[10] Only some of the Working Groups (WGs) of JTC1/SCs or Subcommittees (SCs) of ISO TCs are noted.

Annex E - Identification of Specific "Sub-Items of Work and Their Priorities

Notes:

1. The "sub-items" identified below are based on,

- *the responses of the SC36 P-members to the SC36 N1436 "Survey on Privacy/Data Protection Requirements for Education, Learning and Training";*
- *further work by the JTC1/SC36 Ad-Hoc on Privacy; and*
- *those identified by JTC1/SC36/WG3 at its September, 2009 Stuttgart Plenary meetings and which were adopted by the JTC1/SC36 as "Resolution 19: (Stuttgart 2008): Privacy issues (see document JTC1/SC36 N1721)*

2. Following adoption of this NWI proposal and its assignment to JTC1/SC36/WG3, the WG3 will determine the most effective manner for grouping the LET privacy issues into defined Parts 2+ of this standard.

E.1 Need for a framework or reference model

Based on the assumption that there will be a multipart standard, the SC36 Ad-Hoc on Privacy (AHP) places a priority on the development of a Part 1: Framework Model or Reference Model.

The focus and purpose of such a Part 1 would include the development of:

- key principles governing the multipart standard including a set of privacy protection principles (high level) such as already identified in the SC36N1436 Survey document and the SC36 AHP N0015 French contribution;

- identification of key concepts and their definitions. (Here some are already found in SC36N1436). In addition, it is anticipated that well over 80%+ of the required concepts and their definitions can be drawn from existing international standards.

- rules governing the addition of subsequent parts.

- development and agreement on a scope statement for the multipart standard as a whole and then within the overall scope statement that for Part 1 in particular.

E.2 Sub-items based on Response to Survey Question 4 – Identification of Types of data in an e-learning context requiring privacy protection

Those identified by SC36 P-members include (in no particular order):

- demographics, age, enrolment information;

- tombstone information, i.e., identity of learner and contact information , including evaluation history (as defined under applicable legislation), evaluation records/ grades, results of assessment (unless released with the consent of the learner);

- education history;

- evaluation records/grades, results of assessment (unless with consent of learner)
- any information pertaining to special accommodations related to the learner, (e.g., hearing impaired, visually impaired, etc.)[11];

- any information pertaining to work experience;

---

[11] Note: There is a link here to the JTC1/SC36 standards development work on the multipart ISO/ IEC 24751 standard.

- any unique identifier(s) for a student;
- any codes (based on coded domain) which indicate personal aspects of an individual including, racial origin, political opinion, religious or other convictions health information, sexual orientation, etc.
- rules about the use/release of student work are sometimes unclear
- those of post-secondary institutions, as per their internal guidelines in support of privacy protection requirements
- all e-learning contexts (e.g. online, televised, etc.) are subject to privacy of student information, i.e., regardless of mode of study
- with increased use of technologies, in learning contexts, especially through social networking and collaborative learning tools, there is an increased ability to record every transaction and interaction. Here more stringent policies on ethics and codes of conduct and more diligent public awareness raising may be a more positive response than one which is technology-based (as technologies keep changing); and,
- with respect to the above the application of privacy protections requirements to electronic data interchange among autonomous parties with respect to personal information of a "LET" nature.

E.3 Sub-items based on Response to Survey Question 5 – Identification of Specific e-Learning Needs pertaining to privacy issues

Those already identified by SC36 P-members are summarized as follows:

- e-learning provided by public sector organizations receives a high degree of privacy protection under legislation. Privacy protection is "IT-neutral", i.e. it pertains to the recorded information on or about an identifiable individual irrespective of the information and communications technologies (ICT) used, i.e., whether recorded or managed in digital or non-digital form;
- personal information regarding students/learners who are "minors" requires added particular/special privacy/data protection. Within Canada, the "default" age of a minor is less than 18 years of age[12].
- certification that qualifies one to perform a certain job
- need for codes of conduct for online course with respect to information sharing by participants (e.g. via social networks such as MySpace, Facebook, wikis, You Tube, blogs, etc.). Here "best practices" in e-learning need to be more broadly promoted and implemented. These and related pedagogical issues could perhaps be supported by appropriate standards.

3.4 Those identified by SC36/WG3 as per JTC1/SC36 Resolution 19: (Stuttgart 2008): Privacy issues (see document JTC1/SC36 N1721)

---

[12] The definition of age of majority, i.e., when an individual is considered to be a "minor" varies within Canadian jurisdictional domains at both the federal and provincial/territorial levels of jurisdictional domains. It also varies with respect to rights and responsibilities of both (1) the individual; and, (2) those of its parent(s) or guardian(s).

“SC36 notes there are privacy issues concerning the following domains that may be within or related to the WG3 scope:

- *Access to mobile learner information, and in particular access to contextual information*
- *Identifying information related to e-portfolios.*
- *Applications of sensor technologies to LET, and in particular, applications to assessments, learner localization, etc.*

This list may not be exhaustive.”

Annex F - Working Definitions and Draft Privacy Protection Principles

Note 1: The text which follows is a cut and paste of Annex B & Annex C [as taken from the JTC1/SC36 Questionnaire document 36N1436 titled "Survey on Privacy/ Data Protection Requirements for Education, Learning and training (LET), a.k.a. "eLearning"]. JTC1/SC36 P-members were asked to comment on these key working definitions as found in Annex B as well as the draft set of Privacy Protection Principles as found in Annex C.

Note 2: The results here can be summarized as follows:

a) no JTC1/SC36 P-member body who responded to the JTC1/SC36 document 36N1436 document had any critical or negative comments on the contents of Annex B and Annex C; and,
b) several responding Ministries of Education provided positive comments on the contents of either this Annex B or Annex C, or both.

Note 3: Consequently, the draft Privacy Protection "working definitions' and principles" as presented below will serve as a basis for the development of the Part 1 Framework/Reference Model for this multipart standards project.

Note 4: It is assumed that as in the development of Part 1 Framework/Reference Model, the final text may be amended as a result of the development of a working draft (WD) and/or subsequent resolution of P-member ballot comments on the CD and/or FCD documents.

Here follows the text of JTC1/SC36 N1438 - Annex B - Working Definitions[13]

1. Why "Privacy/Data Protection" as a name for the Questionnaire?

"Privacy" and "Data Protection" are two of the most common labels given to laws and pursuant regulations in the countries who are members of ISO/IEC JTC1/SC36, or as a matter of fact of all ISO/IEC JTC1 member countries. These legal and/or regulatory requirements apply to "personal information".

2. What is "personal information"?

"Personal information[14]" can be defined as:

> ***personal information:*** *any information on or about an identifiable individual that is recorded in any form including electronically or on paper.*
>
> *NOTE: Some examples would be recorded information about an individual's religion, age, financial transactions, medical history, address or blood type. In some legislation, it may be specifically forbidden to process some types of information.*

3. What is "privacy protection"?

The primary sources of the legal and/or regulatory requirements of a "privacy" or "data protection" requirements nature are jurisdictional domains. Jurisdictional domains can be (1) nation-states, i.e., UN member bodies; or, (2) where the nation-state is of a federated nature, its provinces, states, territories, länder, cantons, etc. A jurisdictional domain may also be of the nature of a "supranational regulatory governance" body such as the European Commission, the European

---

13 These working definitions are used here to help integrate ISO and ISOIEC JTC1 standards development work related to supporting implementation of privacy/data protection requirements.

14 The concept of an "identifiable individual" includes: (1) data which in itself identifies an individual, (e.g., as a record about that individual such as a student record, an assessment, etc.); (2) recorded information resulting from a collaborative or interactive e-learning process which identifies the individual participants; and, (3) the linking of recorded information in one or more disparate information systems to identify an individual, (a.k.a. "data matching", or "data linking", etc.).

Court of Justice, etc.

In the context of "privacy" or "data protection", jurisdictional domains are the primary source of external constraints which govern the creation, collection, use, retention, etc., of recorded information about an identifiable individual by an organization (including public administration). These external constraints of a "privacy" or "data protection" requirements nature, i.e., "privacy protection" can be defined as:

> ***privacy protection:*** *a set of external constraints of exercised by a jurisdictional domain limiting the processing of information on or about an identifiable living individual, i.e., personal information, including creation, collection, management, retention, access and use, and/or distribution of such recorded information*

Here follows the text of JTC1/SC36 N1436 - Annex C - Summary of Privacy/Data Protection Requirements

Although legislation and regulations of a privacy/data protection nature differ among the many jurisdictional domains where they exist, on the whole, they have much more in common. A review and analysis of privacy/data protection legislation in Australia, Canada, Japan, USA (including at the state level), and Norway as well as Europe (both at the EU level, that of countries (e.g. within country such as those of länder within Germany), Sweden, etc., indicates that all these laws and regulations have common requirements.

For the purposes of this questionnaire, these common requirements have been summarized (by ISO/IEC JTC1/SC36) into ten (10) Privacy/Data Protection Principles[15].

Privacy Principle 1: Accountability

An organization[16] is responsible for the governance of personal information under its control and shall designate an organization Person(s) who is/are accountable for the organization's compliance with established privacy principles which in turn are compliant with and support legal requirements of a privacy protection nature of the applicable jurisdictional domain.

Privacy Principle 2: Identifying Purposes

The specified purpose(s) for which personal information is recollected shall be identified by the organization to the individual at or before the personal information is collected.

Privacy Principle 3: Informed Consent

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the explicit informed consent of the individual or as required by law.

Personal information shall be retained only as long as necessary for the fulfilment of the purposes that were consented to.

Privacy Principle 4: Limiting Collection

The collection of personal information shall be limited to that which is solely necessary for the identified and specified purpose(s) of the organization

Principle 5: Limiting, Use, Disclosure and Retention

Personal information shall not be used or disclosed for purposes other than for those it was collected, except with the informed consent of the individual or as required by law. Secondary or derivative uses of personal information are <u>not</u> permitted.

Personal information shall be retained only as long as necessary for the fulfilment of those

---

15 The purpose here is simply to present, in summary form and in a non-technical (or IT-neutral) manner, the key common privacy/data protection. There are other sets of Privacy/Data Protection Principles; some have more and some have less then ten "principles". The same set of requirements can also be grouped differently or have different titles.

16 The use of the term "organization" in these Privacy Principles includes "public administration".

purposes.

Principle 6: Accuracy

Personal information shall be as accurate, complete and up-to-date as is necessary for the specified purposes for which it is to be used.

Principle 7: Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the recorded information and in compliance with such measures as are appropriate to ensure that all applicable legal requirements are supported.

Principle 8: Openness

An organization shall have and make readily available to individuals specific information about its policies and practices pertaining to the management of personal information under its control.

Principle 9: Individual Access

Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information.

An individual shall be able to challenge the accuracy and completeness of his or her personal information and have it amended or deleted as appropriate.

Principle 10: Challenging Compliance

An individual shall be able to address a challenge to an organization concerning its compliance with the above principles to the designated organization Person(s) accountable for the organization's compliance with Privacy requirements, including that interchanged with other organizations (as well as secondary or derivative uses of personal information).

Notes to Privacy Principles

Note 1: Many jurisdictional domains have an "ombudsman", (e.g., a Privacy Commissioner, a Data Protection Commissioner, etc.), who serves as an independent adjudicator of complaints, ensures compliance with privacy/data protection requirements, etc.

Note 2: Most, if not all, jurisdictional domains, which have privacy or data protection laws and/or regulations, also have other laws or regulations which may "override" privacy rights. This and related matters are outside the scope of this JTC1/SC36 Ad-Hoc on Privacy.