FINAL DRAFT

INTERNATIONAL STANDARD

ISO/IEC FDIS 29187-1

ISO/IEC JTC **1**/SC **36**

Secretariat: KATS

Voting begins on:
2016-04-22

Voting terminates on:
2016-06-22

Information technology — Identification of privacy protection requirements pertaining to learning, education and training (LET) —

Part 1: Framework and reference model

Technologies de l'information — Identification des exigences de protection privée concernant l'apprentissage, l'éducation et la formation (AÉF) —

Partie 1: Cadre général et modèle de référence

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/IEC FDIS 29187-1:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 36, *Information technology for learning, education, and training*.

This second edition cancels and replaces the first edition (ISO/IEC 29187-1:2013), of which it constitutes a minor revision.

ISO/IEC 29187 consists of the following parts, under the general title *Information technology — Identification of privacy protection requirements pertaining to learning, education and training (LET):*

— *Part 1: Framework and reference model*

Further parts may be added in the future.

Introduction

Purpose and overview

For the purposes of this part of ISO/IEC 29187, the use of LET covers learning, education and training. In order to determine the need and focus of LET standards in support of privacy protection requirements applicable to personal information of an individual learner, ISO/IEC JTC 1/SC 36 established an "Ad-Hoc on Privacy (AHP)" (the majority of the ISO/IEC JTC 1/SC 36 P-members represent jurisdictional domains which are governed by privacy/data protection requirements of a legislative/regulatory nature which apply to "individual learners). The results of this detailed preparatory work and survey by this JTC 1/SC 36 AHP identified user requirements and served as the basis for the need for this International Standard. See Annex F.

NOTE 1 The mandate and objectives of this JTC 1/SC 36 AHP, as well as the Survey instrument, are stated in document 36N1436.

ISO/IEC JTC 1/SC 36 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 in cases where such standards are used to capture and manage recorded information for 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, human rights, etc.

The role of ISO/IEC JTC 1/SC 36 is to develop ICT-based standards in the fields of learning, education and training (LET). Since the application and use of a majority of JTC 1/SC 36 standards involve the role of an individual as "learner", i.e. as an "individual learner", this means that any recorded information on or about an identifiable individual as a "learner" is subject to applicable privacy/data protection a requirement.

This part of ISO/IEC 29187 serves as a "Framework and Reference Model". Based on a set of (primary) principles, the "Framework and Reference Model" is composed of a number of conceptual and structural models. These are represented via "illustrative" figures and associated lexical models in the form of rules.

NOTE 2 One such lexical model is the key concepts and their definitions of the Framework and Reference Model as presented in Clause 3.

More specific and detailed "typical models" are to be developed in future parts of this International Standard. These future parts will focus on more detailed specifications of particular components of the Framework and Reference Model.

Benefits of using a multipart ISO/IEC 29187 standard approach

There are several benefits from taking an integrated approach.

- A multipart standard approach provides for a systematic, cost-efficient and effective approach to the creation of robust, (re-)useable components in support of LET privacy protection requirements, including those needed to facilitate the use of generic global requirements perspective, as well as added requirements of particular jurisdictional domains of human interface equivalents (HIEs) at any level of granularity.
- This multipart standard will provide cost savings to those organizations and public administrations, individual learners and suppliers of LET-based products and services, i.e. "LET providers". It will do so from a multilingual requirements perspective and in support of cultural adaptability, individual accessibility and diversity.

  NOTE 3 Multilingual communications (whatever the supporting IT platform used including the Internet) is already supported by existing technologies. Many ISO/IEC and ISO standards already exist (or are under development) whose contents can and will be used as building blocks for the integration of this new LET standard.

— having a common IT-facilitated approach will (a) benefit individual users world-wide (doing so in respect and support of cultural diversity), (b) ensure that requirements of jurisdictional domains (at whatever level) can be supported in a very cost-effective and efficient manner, and (c) also benefit suppliers of LET focused products and services.

The concept of (semantic) collaboration space (SCS), introduced in Clause 7 is directed at supporting the implementation of the *UN Convention on the Rights of Persons with Disabilities* in an ITLET context including those of a privacy protection nature.

Informed consent and learning transaction

NOTE 4 Annex E provides informative information on the key modelling constructs introduced in this part of ISO/IEC 29187.

A key privacy protection requirement is that it requires informed consent of the individual, including in the role of an individual learner. It also requires the identification of the purpose(s), goal for which the personal information is to be created/collected, used, managed, shared, deleted, etc. In addition to identifying purpose(s) and informed consent (presented below) as Privacy Protection principles in 5.3.3 and 5.3.4, there are also the Privacy Protection Principles of "accountability" of "limiting collection", "limiting use, disclosure and retention", "accuracy", "openness", "individual access", and "challenging compliance" (presented below Privacy Protection principles in 5.3.2, 5.3.5, 5.3.6, 5.3.7, 5.3.9, 5.3.10, and 5.3.11, respectively).

Requirements of this nature focus on what might be considered the LET operational view (LOV). In addition, there are ICT technical support requirements for privacy protection principles #8 "safeguards" (see 5.3.8). These include security services, communication services, etc.

Requirements of this nature are not unique to an LET (or ITLET) context. They have already been identified and addressed in a generic manner in the ISO/IEC 14662 Open-edi Reference Model as being a "transaction" nature in support of an agreed upon commitment exchange between an individual learner and an LET provider.

Consequently, the "LET Privacy Protection Framework and Reference Model" (presented in Figure 1) is based on the "Open-edi Reference Model". A key construct of the Open-edi Reference Model is that it recognizes that a commitment exchange, modelled as a transaction needs to be treated and supported as a whole. At the same time, and from an ICT (including ITLET) perspective, it is recognized that ICT-based support services, i.e. functional support services view change as ICT changes on the whole, but those of the user and operational requirements view remain fairly constant. The interaction and inter-working between (a) the user operational view and (b) the ICT support services view in modelling a transaction and then developing standards in support of the same as presented in the Open-edi Reference Model as the need to differentiate between the business operation view (BOV) and functional services view (FSV) (see Annex E). LET privacy protection Framework and Reference Model uses these two views of the Open-edi Reference Model to describe the relevant aspects of a learning transaction:

a) the "Learning Operational View (LOV) aspects of a learning transaction;

b) the "LET- FSV view of a learning transaction.

The Learning Operational View (LOV) addresses the aspects of the context and semantic aspects of personal information in a learning transaction including data management and interchange aspects. The LOV also can be referred to as the operational and user requirements view.

The LET-FSV addresses the ICT infrastructure and support services meeting the mechanical needs of the Learning Operational View. Its purpose is to support the demands on the supporting ICT infrastructure of the Learning Operational View. It focuses on ICT aspects of

a) functional capabilities,

b) service interfaces, and

c) protocols and APIs.

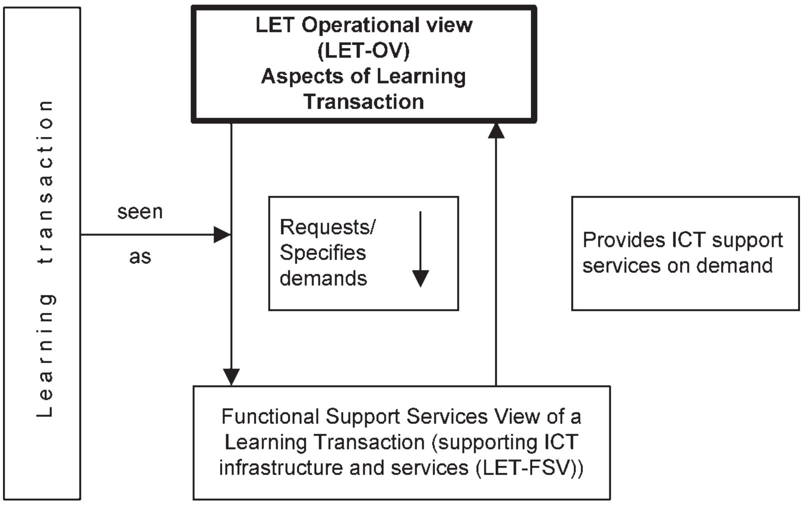

Figure 1 — Learning Transaction — Privacy Protection — Framework and Reference Model

Use of "jurisdictional domain", jurisdiction, country

NOTE 5 For more detailed information on this and related matters pertaining to "jurisdictional domain", see ISO/IEC 15944-5. This is a freely available ISO/IEC standard (see http://standards.iso.org/ittf/PubliclyAvailableStandards/).

Multiple different definitions are currently in use for "jurisdiction". Some have legal status and others do not. Further, it is a common practice to equate "jurisdiction" with "country". Yet, at the time, it is also a common practice to refer to "provinces", "states", "länder", "cantons", "territories", "municipalities", etc., as jurisdictions. In addition, several UN member states can combine to form a "jurisdiction" (e.g. the European Union, NAFTA, etc.).

In this standard,

a) the use of "jurisdictional domain" represents its use as a defined term, and

b) the use of "jurisdiction(s)" and/or country(ies) represents their use in generic contexts.

Most often in this International Standard, "jurisdictional domain" is used as it represents the primary source of external constraints pertaining to "privacy protection" rights of individuals. It also reflects the fact that in UN member states which are "federated" in nature, that it is the "province", "state", "länder", "territory", in that UN member state which is often responsible for LET-related activities and thus is the responsible jurisdictional domain.

This International Standard incorporates the common aspects of such laws and regulations as pertaining to privacy protection, applicable at the time of publication only. The concept of "privacy protection" also integrates these various set of legal and regulatory requirements and does so from a public policy requirements perspective. See Clause 7

It has to be born in mind that the delivery of "privacy protection" requires action both at the LET operational level (LOV) and technology level of functional service (FSV). Where human beings interact with recorded information once it has passed through an Open-edi transaction, they may have the potential to compromise technical controls (FSV) that may have been applied. It is essential that LET models take account of the need to establish overarching operational processes that address issues that have not been, and/or cannot be resolved by the technical FSV controls applied so as to provide the overall privacy demands of regulation that should be applied to personal data, their use, proscribed dissemination and so on. In this regard, the interplay of the LOVLOV and FSV views of all organizations should be taken into account.

Use of "Person", "individual", "organization", "public administration" and "person" in the context of a learning transaction

It is important to differentiate an "individual" from the other two sub-types of Person, namely that of an "organization" and a "public administration". There are several reasons why this is necessary. These include the following.

a) The fact that in UN conventions, Charters, treaties, etc., as well as in the laws and regulations of jurisdictional domains, the word "person" is often used without explicitly specifying whether "person" applies only to a human being, a natural person, i.e. as an "individual," but also other types of persons recognized in law, i.e. legal persons such as organizations and public administrations.

   NOTE 6 The "*UN Convention on the Rights of Persons with Disabilities*" does not explicitly state or define what a "Person" is. From its purpose and context, one deduces that these are "natural persons" and not "legal persons" (e.g. not organizations or public administrations). In an ICT environment (or the virtual world), one needs to be very explicit.

   For example, the human right of "freedom of expression" which is stated in the UN Charter as written and was intended to be a right of human beings (natural persons) only. However, in some well as the Constitution (and/or Charter of Human Rights) and of most jurisdictional domains was jurisdictional domains, corporations have been allowed to claim the right of "freedom of expression" since they are also "Persons", i.e. "legal persons", with the result that "freedom of expression" rights are applied to "advertising".

b) The need to ensure that public policy requirements of jurisdictional domains (see Clause 6 below) which are created and intended for human beings continue to pertain to human beings only, i.e. "individual".

c) For the first 20 years to 30 years, the use of ICT was restricted to organizations and public administrations. The advent of the Internet and the World-Wide Web (WWW) has resulted in "individuals" becoming full participants in the use of ICT.

Consequently, many, if not most of the ISO/IEC JTC 1 standards, as well as other ICT-based standards of ISO, IEC and ITU (and others) do not distinguish whether or not the real end user is another IT system or a Person, i.e. an entity able to make a commitment, and then whether that entity making a commitment is doing so on behalf of itself, i.e. as an "individual", or on behalf of an organization, i.e. as an organization Person.

To address these and other related requirements, the additional concept and term of "Person" was introduced and defined (see ISO/IEC 15944-1:2011, 6.2) in such a way that it is capable of having the potential legal and regulatory constraints applied to it, i.e. as "external constraints". In the context of this International Standard, these include the following:

a) external constraints of a public policy nature in general and of a "privacy protection" nature in particular as legal rights of an individual;

b) external constraints of a public policy nature in general and of a privacy protection nature in particular, which apply to organizations or public administrations as legal obligations to be complied with when providing goods and services to any individual.

In summary, there are three broad categories of a Person as a player in any process involving the making of a decision, and/or the making of a "commitment" namely the following:

a) the Person as "individual";

b) the Person as "organization";

c) the Person as "public administration".

There are also three basic (or primitive) roles of Persons in learning transactions, i.e. the making of a commitment of whatever nature, namely "buyer", "seller", and "regulator".

The reader of this International Standard should understand that

a) the use of Person with a capital “P” represents Person as a defined term, i.e. as the entity that carries the legal responsibility for making commitment(s),

b) “individual”, “organization” and “public administration” are defined terms representing the three common sub-types of “Person”, and

c) the words “person(s)” and/or “party(ies)” are used in their generic contexts independent of roles of “Person” (as defined in ISO/IEC 14662 and ISO/IEC 15944-1). A “party” to any decision making process, a commitment making process (including any kind of learning transaction) has the properties and behaviours of a “Person”.

Importance of definitions and terms

NOTE 7 See further, the document titled *“Importance of Definitions for Concepts”,* (2008-05-20) ISO/IEC JTC 1 N0129/SC 36.

The ISO/IEC Directives Part 2 provide for “Terms and definitions” as a “Technical normative element”, necessary for the understanding of certain terms used in the document. A primary reason for having “Terms and definitions” in an International Standard is because one cannot assume that there exists a common understanding, worldwide, for a specific concept. And even if one assumes that such an understanding exists, then having such a common definition in Clause 3 serves to formally and explicitly affirm (re-affirm) such a common understanding, i.e. ensure that all parties concerned share this common understanding as stated through the text of the definitions in Clause3.

A primary objective of the ISO/IEC 29187-1 standard on LET privacy protection is the need

a) to have clear, unambiguous and explicitly stated definitions for the concepts introduced or used,

b) to appreciate and understand that one needs to be careful in the choice of the “label”, i.e. term, to be associated with a concept, and

c) to understand that a) and b) are essential to privacy protection and the creation and provision of human interface equivalents (HIEs) of the semantics of the content of what is intended to be communicated. This is required to support the “informed consent” privacy protection requirement.

If one looks at any UN convention, treaty, covenant, any law or regulation of a jurisdictional domain, an International Standard, etc., one will find that their first two chapters, clauses, articles or sections are “purpose” or “scope” and “definitions”. From an academic and scientific LET perspective, the introduction of a new concept, its definition, what it “is” (or meant to be understood as), how and where it fits or is to be used, etc., is the focus of many papers, presentations, etc.

Definitions of concepts form the foundation of research and even more so in a multidisciplinary network context. As such, it is important that definitions be explicit, unambiguous, and precise with respect to the semantics conveyed.

This is important because the “definition” and associated label, i.e. “term”, of a concept not only serves as the basis for a “common understanding” of all parties involved but also serves as the basis for any other (non-involved) individual to be able to understand the meaning and use of a concept as per its definition and a common bridge between ICT-based and ICT-neutral approaches.

At times, in order to ensure that the concept being defined is not confused with other related concepts, i.e. via word, label, or term, used to denote the concept, it is necessary to introduce, i.e. invent or “coin”, a new term as the label for that concept. The key purpose is not to have multiple different meanings associated with a single label or term.

Standard based on rules and guidelines

This standard is intended to be used within and outside of the ISO, IEC, and ITU communities by diverse sets of users having different perspectives and needs.

ISO states (ISO/IEC JTC 1 Directives, Part 1: 1998, 2.5 and ISO/IEC Guide 2:2004, 1.7) that a new standard is a

"documented agreement containing technical specifications or other precise criteria to be used consistently as rules, guidelines, or definitions of characteristics to ensure that materials, products, processes and services are fit for their purpose".

This International Standard focuses on "other precise criteria to be used consistently as rules, guidelines or definitions of characteristics, to ensure that products, processes and services are fit for their purpose", i.e. from an operational and user perspective by individuals and in compliance with applicable external constraints.

This means that this International Standard is based on rules which are predefined and mutually agreed to. See Clause 5 and succeeding clauses.

Size of document and role of this part of ISO/IEC 29187

While in an ITLET context, this part of ISO/IEC 29187 may seem to be voluminous, it is noted that there are many ISO/IEC JTC 1 (and ISO or IEC) standards which are over 1,000 pages in size. The purpose of this part of ISO/IEC 29187 is exactly that, to provide an overall "Framework and Reference Model" in an ITLET context to identify the requirements and context for implementation of these requirements in subsequent Parts of ISO/IEC 29187.

In order for subsequent parts of this multipart standard to be as "short" as possible, it is necessary for them to be able to use and reference normative and informative Clauses and Annexes of this part of ISO/IEC 29187.

Use of "identifier" (in a learning transaction)

Unambiguous identification of the two primary parties to a learning transaction, i.e. the individual learner and the LET provider (as well as associated agents or third parties) is a primary LET privacy protection requirement. Clause 8 and Clause 11 addresses the issues pertaining to the establishment and management of use of identities of parties to a learning transaction, that of the parties to a learning transaction (including the use of various personae (or names) identities, etc.

However, "unambiguous" is a key issue in learning transactions because states of unambiguity and uncertainty are not permitted in the context of LET privacy requirements and even more so with respect to LET transactions which involve EDI. A key assumption of Open-edi Reference Model which applies to any commitment made among autonomous parties is that the resulting transaction shall have a unique identifier.

Use of "privacy protection" in the context of a commitment exchange and learning transaction

To be able to address privacy protection requirements, one needs to do this in the context of a commitment exchange between an individual learner and an LET provider involving identified purpose and informed consent. Such a set of activities is modelled as a learning transaction, i.e. a set of activities or processes which is initiated either by an individual learner or an LET provider to accomplish and explicitly shared goal and terminated upon recognition of one of the agreed conclusions by all the involved Persons, although some of the recognition may be implicit (e.g. a student drops out of a class or a study programme).

Organization and description of document

This part of ISO/IEC 29187 identifies basic common LET privacy protection requirements, as external constraints of jurisdictional domains, on the modelling of learning transactions.

Introduction provides key concepts and common content for this multipart standard. These are based on ISO/IEC 14662, as well as the ISO/IEC 15944 series.

Clause 1, which follows, not only provides the overall scope of this part of ISO/IEC 29187 but this states its exclusions, as well as relevant aspects not yet addressed in this edition of this part of ISO/IEC 29187.

Clause 2 provides the Normative References used in this part of ISO/IEC 29187. It is noted that a key principle in the development of this par of ISO/IEC 29187 (as well as subsequent Parts) is to maximize use of existing international ISO, ISO/IEC, JTC 1, IEC, and ITU-T standards, as well as applicable referenced specifications.

The principle of maximizes re-use of applicable international standards also applies to subsequent Clause 3 and Clause 4.

Clause 5 provides the key elements applicable to not only this part of ISO/IEC 29187 but all other subsequent Parts of ISO/IEC 29187. Clause 5 identifies the fundamental principles governing privacy protection requirements on learning transactions involving individual learners.

The purpose of Clause 6 is to place the Clause 5 privacy protection requirements identified as "Fundamental Principles" in Clause 5 in the context of the use of the "collaboration space" modelling construct" in support of privacy protection requirements. The focus of Clause 6 is to place LET privacy protection requirements in a "collaboration space" context. The purpose is recognition and support of the fact that the "identifying purpose" and "informed consent" LET privacy protection requirements (see 5.3.3 and 5.3.4). Clause 6 introduces the concept of "learning collaboration space" and does so in the context of a "learning transaction".

The purpose of Clause 7 is to situate LET privacy protection requirements in the context of other similar public policy requirements such as consumer protection and individual accessibility.

Clause 8 focuses on presenting the principles and rules governing the management of use of identities of an individual learner. Based on generic Open-edi standards, it brings to the fore the fact of an individual having multiple personae, identities, associated unique identifiers, legally recognized individual identities, etc.

Clause 9 introduces the Person components focusing on the individual (learner) sub-type. It addresses issues such as rule qualification, legally recognized names, truncation of names, as well as anonymization and pseudonymization.

The five fundamental activities comprising the Process component of a learning transaction are introduced in Clause 10. They are planning, identification, negotiation, actualization and post-actualization.

The data (element) component of a learning transaction are presented in Clause 11. This Clause includes sets of rules governing the role of a Learning Transaction Identifier (LIT), those pertaining to change management, as well as records retention of the SRIs in the learning transaction. Clause 11 concludes with h a set of rules governing date/time referencing.

Clause 12 provides two types of Conformance Statements, namely one which pertains to ISO/IEC 29187-1 Reference Mode and one which applies to Conformance with any of the future parts of ISO/IEC 29187.

At the end of this part of ISO/IEC 29187 are some helpful annexes that provide elaboration, as well as normative references in the main body. Normative annexes include Annex "A", which is a consolidated list of the definitions found in Clause 3 presented in matrix form of ISO English and ISO French equivalents.

Other normative Annexes include Annex B which brings forward key aspects of the Learning transaction model (LTM) and classes of constraints. Annex C provides, in summary form, the applicable set of information life cycle management principles (ILCM), while Annex D focuses on presenting coded domains for specifying state changes and records management decisions in support of privacy protection requirements.

Annex E provides added informative information on the Open-edi Reference Model. Annex F provides information on the results of the JTC 1/SC 36 Ad-Hoc on Privacy (AHP) including the identification of potential future parts of ISO/IEC 29187, as well as those resulting from the developments of this part of ISO/IEC 29187-1.

Information technology — Identification of privacy protection requirements pertaining to learning, education and training (LET) —

Part 1:
Framework and reference model

1 Scope

1.1 Statement of scope — ISO/IEC 29187 series

The ISO/IEC 29187 series focuses on the identification of privacy protection requirements which apply to any JTC 1/SC 36 ITLET standard or LET activity which involves the following:

a) the identification of an individual (e.g. as a learner or student, a teacher, professor, or instructor, an administrator, etc.), in the use and implementation of the JTC 1/SC 36 standard;

b) any standard which involves the recording of any information on or about an identifiable individual by any LET provider.

1.2 Statement of scope — this part of ISO/IEC 29187

This part of ISO/IEC 29187 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 (LET). The LET transaction – Privacy Protection – Framework and Reference Model is learning transaction focused, rule-based, and conformant to the generic ISO/IEC Open-edi Reference Model. It maximizes re-use of existing ISO standards including applicable concepts and their definitions. LET privacy protection requirements are placed in the generic context of applicable public policy requirements, those pertaining to establishment and management of identities of an individual learner, as well as state changes and records retention requirements of personal information on or about an individual learner. This part of ISO/IEC 29187 also incorporates best practices and policies as have already been implemented in LET environments in support of privacy protection requirements.

1.3 Exclusions

1.3.1 Functional services view (FSV)

This part of ISO/IEC 29187 focuses on the Learning Operational View (LOV) aspects of a learning transaction and does not concern itself with the technical mechanisms needed to achieve the learning requirements. In an LET context, the FSV definition of the LET functional services view (or LET-FSV) is as follows (see 3.76):

*perspective of **learning transactions** limited to those information technology interoperability aspects of **IT Systems** needed to support the execution of Open-edi transactions*

NOTE Adapted from ISO/IEC 14662.

Various LET-FSV aspects include the specification of requirements of a Functional Services Support View (LET-FSV) nature which include security techniques and services, communication protocols, etc. This includes any existing standard (or standards development of an FSV nature), which has been ratified by existing ISO, IEC, UN/ECE and/or ITU standards.

1.3.2 Overlap of and/or conflict among jurisdictional domains as sources of privacy protection requirements

A learning transaction requires an exchange of commitments among autonomous parties, i.e. an individual learner, an LET provider. Commitment is the making or accepting of a right, an obligation, liability or responsibility by a Person. In the context of a learning transaction, the making of commitments pertains to the transfer of an LET good, service and/or right among the Persons involved. In the past and still to a large extent today, the individual learner and the LET provider share the same jurisdictional domain. The advent of the Internet, online, distance, mobile, etc., learning has the result that parties to a learning transaction are often located in differing jurisdictional domains.

Consequently, it is not an uncommon occurrence depending on the goal and nature of the learning transaction that the Persons (and parties associated) are in different jurisdictional domains, and that, therefore, multiple sets of external constraints apply and overlap will occur. It is also not an uncommon occurrence that there is overlap among such sets of external constraints and/or conflict among them. This is also the case with respect to laws and regulations of a privacy protection nature. Resolving issues of this nature is outside the scope of this part of ISO/IEC 29187.

However, the modelling of learning transaction as scenarios and scenario components as re-useable business objects may well serve as a useful methodology for identifying specific overlaps and conflicts (thereby serving as a tool for their harmonization).

As such, the Open-edi descriptive techniques methodologies and constructs, can serve as a tool in harmonization and simplification of external constraints arising from jurisdictional domains.

NOTE This edition of this part of ISO/IEC 29187 is based on the following assumptions:

a) the privacy protection requirements of the individual learner, as a buyer in a learning transaction, are those of the jurisdictional domain in which the individual made the commitments associated with the instantiated learning transaction;

b) where the LET provider is in a jurisdictional domain other than that of the individual leaner, this edition of this part of ISO/IEC 29187 incorporates and supports the generic common privacy protection requirements which are expressed in eleven principles in Clause 5.

1.3.3 Publicly available personal information

Excluded from the scope of this part of ISO/IEC 29187 are personal information which are publicly available, i.e. “publicly available personal information. In a learning transaction context, the LET provider does not collect personal information of this nature from the individual (particularly in the “planning phase” of the learning transaction process).

For example, the LET provider in advertising a new LET product or service to the market may access and use the following:

a) public personal information, i.e. publicly available personal information such as that found in telephone directories;

b) any personal information declared to be of a public information by a regular based on an law or regulation of the applicable jurisdictional domain;

c) that which the individual itself to make public (e.g. via one or more Internet-based applications such as “Facebook”, Twitter, letters to the editor, etc. These also include those applications where the individual decides not to invoke or use available “privacy settings”.

In a privacy protection context, publicly available personal information (PAPI) is defined as follows:

***personal information** about an **individual** that the **individual** knowingly makes or permits to be made available to the public, or is legally obtained and accessed from (a) government records that are available to the public or (b) information required by law to be made available to the public*

EXAMPLE 1 Personal information which an individual knowingly makes or permits to be made available include public telephone directories, advertisements in newspapers, published materials, postings of this nature on the internet, etc.

EXAMPLE 2 Government records that are publicly available include registers of individuals who are entitled to vote, buy or sell a property, or any other personal information that a jurisdictional domain requires to be publicly available, etc.

Further, determining whether or not personal information is of a publicly available information nature is also excluded from the scope of this part of ISO/IEC 29187.

1.4 Aspects currently not addressed

NOTE 1 See also Annex F, which focuses on the identification of user requriements for additional future aprts based on this part of ISO/IEC 29187.

This edition of this part of ISO/IEC 29187 focuses on the essential, i.e. generic and primitive, aspects only. The purpose of this Clause is to identify aspects not currently addressed. These will be addressed in either of the following:

a) an Addendum to this part of ISO/IEC 29187;

b) the third edition of this part of ISO/IEC 29187;

c) through a new Part of the ISO/IEC 29187 series;

d) in a new International Standard.

In this context, this edition of this part of ISO/IEC 29187 does not currently support the following requirements.

a) The differences in equality in use of official languages by an individual, in being informed and exercising privacy protection rights within a jurisdictional domain.

   NOTE 2 This part of ISO/IEC 29187 focuses on the essential basic, i.e. primitive, aspect of jurisdictional domains as sources of external constraints. As such, this second edition of this part of ISO/IEC 29187 does not address differences in status that can exist among official languages within a jurisdictional domain. It is not uncommon that where a jurisdictional domain has three or more official languages that not all of these have equal status. For example, for use of some official language(s) in a jurisdictional domain, there could be criteria such as “where and when numbers warrant”, “there is a significant demand for communication with and services from a public administration in that language”, etc. This impacts both the language in which personal information is recorded by an organization or public administration, as well as the language of communications of the individual with the organization in a learning transaction.

b) The interworking between privacy protection and consumer protection requirements as two sets of external constraints applicable to an individual as a buyer in a learning transaction.

c) The identification and registration of schemas involving the control and management of legally recognized names (LRNs) as personas and associated unique identifiers for the unambiguous identification of an individual and/or the role qualification of an individual learner in a specific context.

d) The more detailed information management and audit requirements pertaining to ensuring privacy protection of personal information that should be enacted by and among organizations and public administrations as parties to a learning transaction.

e) The more detailed rules and associated text pertaining to the learning operational view perspective with respect to transborder data flows of personal information.