INTERNATIONAL STANDARD

ISO/IEC 29187-1

First edition
2013-02-15

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

Reference number
ISO/IEC 29187-1:2013(E)

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

Published in Switzerland

Contents

Page

Figures

Tables

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.

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

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

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

ISO/IEC 29187-1 was prepared by Joint Technical Committee ISO/IEC JTC1, *Information technology*, Subcommittee SC 36, *Information technology for learning, education, and training*.

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.

[THIS PAGE IS INTENTIONALLY LEFT BLANK]

0 Introduction

0.1 Purpose and overview

For the purposes of this standard, 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 JTC1/SC36 established an "Ad-Hoc on Privacy (AHP)"[1] The results of this detailed preparatory work and survey by this JTC1/SC36 AHP the identified user requirements and serve as the basis for the need for this multipart standard[2] {See further Annex F below}

ISO/IEC 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 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 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", 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.

ISO/IEC 29187-1 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[3] in the form of rules.

More specific and detailed "typical models" are to be developed in Parts 2+ of this multipart standard. These Part 2+ will focus on more detailed specifications of particular components of the Framework and Reference Model.

0.2 Benefits of using a multipart ISO/IEC 29187 standard approach

There are several benefits from taking an integrated approach: First, 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.

---

[1] The majority of JTC1/SC36 P-members represent jurisdictional domains which are governed by privacy/data protection requirements of a legislative/regulatory nature which apply to "individual learners

[2] The mandate and objectives of this JTC1/SC36 AHP as well as the Survey instrument are stated in document 36N1436

[3] One such lexical model is the key concepts and their definitions of the Framework and Reference Model as presented in Clause 3.0 below.

Second, 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[4)] perspective and in support of cultural adaptability, individual accessibility and diversity.

Third, having a common IT-facilitated approach will: (1) 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, (3) also benefit suppliers of LET focused products and services.

The concept of (semantic) collaboration space (SCS), introduced in Clause 7 below 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.

0.3 Informed consent and learning transaction [5)]

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 Clauses 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 Clauses 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 (LET-OV). In addition, there are ICT technical support requirements for privacy protection principles #8 "safeguards" (see Clause 5.3.8 below). These include security services, communication services, etc.

Requirements of this nature are not unique to a 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 a LET provider.

Consequently, the "LET Privacy Protection Framework and Reference Model" (presented below 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 9is recognized that ICT-based support service, 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. This operation between the user view and the ICT view in modelling a transaction and developing standards in support of the same is presented in the Open-edi Reference Model as the need to differentiate between the business operation view (BOV) and functional services view (FSV).[6)] 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 (LET-OV) aspects of a learning transaction; and,

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

---

4) 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.

5) Annex E below "Open-edi Reference Model and Learning transaction" provides informative information on the key modelling constructs introduced in ISO/IEC 29187-1.

6) See further below, Annex E (informative) titled "*Use and adaptation of the Open-edi Reference Model".*

The Learning Operational View addresses the aspects of the context and semantic aspects of personal information in a learning transaction including data management and interchange aspects. The LET-OV 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;

c) protocols and APIs.

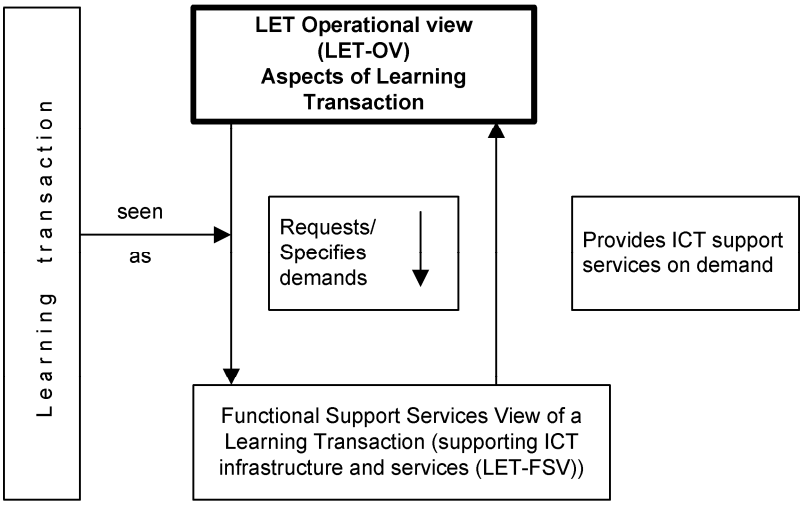

Figure 1 — Learning Transaction - Privacy Protection – Framework and Reference Model

0.4 Use of "jurisdictional domain", jurisdiction, country[7)]

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 document “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.

[7)] For more detailed information on this and related matters pertaining to “jurisdictional domain”, see ISO/IEC 15944-5:2008 (E) *Information Technology - Business Operational View - Part 5: Identification and referencing of requirements of jurisdictional domains as sources of external constraints.* This is a freely available ISO/IEC standard.

This 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 below Clause 7}

It has to be born in mind that the delivery of "privacy protection" requires action both at the LET operational level (LET-OV) 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 must be applied to personal data, their use, proscribed dissemination and so on. In this regard, the interplay of the LET-OV and FSV views of all organizations must be taken into account.

0.5 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:

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 here "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[8)]

   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 further 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 20-30 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 JTC1 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: (a) another IT system; or, (b) 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.

---

8) The "U*N 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 here.

To address these and related requirements, the additional concept and term of "Person" was introduced and defined[9] 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 standard, these include:

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

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: (1) the Person as "individual"; (2) the Person as "organization"; and, (3) 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 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 the ISO/IEC 14662:2010 and ISO/IEC 15944-1 standards). 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".

0.6 Importance of definitions and terms[10]

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 a 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 Clause 3.

---

[9] See further Clause 6.2 "Rules Governing the Person component" in ISO/IEC 15944-1:2010 (3rd ed.) titled "Information technology – Business operational view – Part 1: Operational Aspects of Open-edi for implementation". [The multipart ISO/IEC 15944 eBusiness standard, as well as the ISO/IEC 14662 Open-edi Reference Model standard, are "publicly available" ISO standards, see http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

[10] See further, the document titled *"Importance of Definitions for Concepts",* (2008-05-20) SC36/WG7 N0129.

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

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

2) 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,

3) to understand that (1) and (2) 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: (1) "purpose" or "scope", and, (2) "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:

1) serves as the basis for a "common understanding" of all parties involved; but also,

2) serves as the basis for (a) any other (non-involved) individual to be able to understand the meaning and use of a concept as per its definition; and, (b) 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 here is not to have multiple different meanings associated with a single label or term.

0.7 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 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 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 standard is based on rules which are predefined and mutually agreed to. {See further Clause 5+ below}

0.8 Size of document and role of "*Part 1 Framework and Reference Model"*

While in an ITLET context, this Part 1 of ISO/IEC 29187 may seem to be voluminous, it is noted that there are many ISO/IEC JTC1 (and ISO or IEC) standards which are over 1,000 pages in size. The purpose of this "Part 1 Framework and Reference Model" 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 this multipart standard.

In order that subsequent Parts 2+ of this multipart standard can 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 1 document.

0.9 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. Clauses 8 and 11 below 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.

0.10 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 among an individual learner and a 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 a 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).

0.11 Organization and description of document

The ISO/IEC 29187-1 Framework and Reference Model standard identifies basic common LET privacy protection requirements, as external constraints of jurisdictional domains, on the modelling of learning transactions.

Clauses 0.1 – 0.n provide key concepts and common content for this multipart standard. (These are based on the ISO/IEC 14662:2010 Open-edi Reference Model as well as the multipart ISO/IEC 15944 standard).

Clause 1 Scope, which follows, not only provides the overall scope of this multipart standard, including that of "Part 1: Framework and Reference Model" but this states its exclusions as well as relevant aspects not yet addressed in this 1st edition of the Framework and Reference Model.

Clause 2 provides the Normative References used in this document. It is noted that a key principle in the development of ISO/IEC 29187-1 (as well as subsequent Parts) is to maximize use of existing international ISO, ISO/IEC, JTC1, 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 "Definitions" and Clause 4 "Symbols and abbreviations".

Clause 5 provides the key elements applicable to not only this Part 1 but all other subsequent Parts of this multipart standard. 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 here is recognition and support of the fact that the "identifying purpose" and "informed consent" LET privacy protection requirements. {See further below Clauses 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 (1) which pertains to ISO/IEC 29187-1 Reference Mode; and, (2) one which applies to Conformance with any of the Parts 2+ of this multipart standard.

At the end of this document are some helpful Annexes that provide elaboration as well as normative references in the main body. Normative references 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 beings forward key aspects of the Learning transaction model (LTM) and classes of constraints. Normative Annex C provides, in summary form, the applicable set of information life cycle management principles (ILCM), while normative 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 (informative) provides information on the results of the JTC1/SC36 Ad-Hoc on Privacy (AHP) including the identification of potential Parts 2+ in the further development of this multipart standard as well as those resulting from the developments of ISO/IEC 29187-1 standard.

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 multipart standard

This (multipart) standard focuses on the identification of privacy protection requirements which apply to any JTC1/SC36 ITLET standard or LET activity which involves:

1) 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 JTC1/SC36 standard; and/or,

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

1.2 Statement of scope – part 1: Framework and Reference Model

Part 1 of this (multipart) 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 (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 standard 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 standard 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 a LET context, the FSV definition of the LET functional services view (or LET-FSV) is as follows:

> *perspective of **learning transactions** limited to those information technology interoperability aspects of **IT Systems** needed to support the execution of Open-edi transaction*s
>
> *[adapted from ISO/IEC 14662:2004, 3.10]*

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 have 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, a 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 a 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 standard.

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 1st edition of Part 1 is based on the following assumptions:

1) 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; and,

2) where the LET provider is in a jurisdictional domain other than that of the individual leaner, this 1st edition of Part 8 incorporates and supports the generic common privacy protection requirements which are expressed in eleven principles in Clause 5 below.

1.3.3 Publicly available personal information

Excluded from the scope of this standard personal information which is 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;

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

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

3) 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 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 Examples of 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 Examples of 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 standard.

1.4 Aspects currently not addressed[11)]

This 1st edition of ISO/IEC 29187-1 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 either:

1) in an Addendum to this standard;

2) in the 2nd edition of this standard;

3) through a new Part of this multipart standard; and/or

4) in a new ISO standard.

In this context, this 1st edition of ISO/IEC 29187-1 does not currently support the following requirements:

1) the differences in equality in use of official languages by an individual, in being informed and exercising privacy protection rights within a jurisdictional domain[12)]

2) 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;

3) 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;

4) 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;

[11)] See also below Annex F (informative) “Potential Parts 2+ for ISO/IEC 29187 based on results of the ISO/IEC JTC1/SC36 Ad-Hoc on Privacy (AHP). This Annex F focuses on the identification of user requirements for additional Parts 2+ based on this Part 1 Framework and Reference Model.

[12)] Part 8 focuses on the essential basic, i.e. primitive, aspect of jurisdictional domains as sources of external constraints. As such this edition of ISO/IEC 15944-8 does not address differences in status that may 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.

5) the more detailed rules and associated text pertaining to the learning operational view perspective with respect to transborder data flows of personal information[13)]

6) interoperation between jurisdictional domains where they do not possess defined equivalents to their privacy protection requirements or where privacy protection requirements are simply different.

7) the possible application of privacy protection requirements to personal information of an individual once deceased. On the whole, privacy protection requirements do not apply to an individual after his/her death. However, from a learning transaction perspective there may be some continuity in privacy protection requirements, (e.g., those pertaining to temporal aspects of post-actualization aspects of an instantiated learning transaction, (e.g., health care matters, warranties on products, service contracts, rights (including IP), etc.).

NOTE 1 This may also include a settlement of wills, probate, investments, etc., pertaining to that individual once deceased or obligations of a LET provider to return "personal information" and a decrease "individual learner, (e.g., "student record", granting of a degree, etc.)

NOTE 2 Tax information filed has 4-6 records retention requirements in most jurisdictional domains. In some jurisdictional domains, tax matters are confidential and in others they are public. The status of personal information may change as a result of litigation.

NOTE 3 Instantiated learning transactions not only may require personal information to be required to be retained but continue to be protected following the death of an individual, (e.g., many credit card agreements exist after the death of the credit card holder) the medical or psychological record of an individual learner.

NOTE 4 As such, one may need to have an added Clause on privacy protection of personal information on individuals upon death of that individual (with most of these added requirements being addressed in the 2nd edition of Part 1).

8) personal information found in journalistic reports

Not yet addressed in this 1st edition of Part 1 is the use of personal information in a learning transaction which is found in journalistic reports including news items, public broadcasts, items published by news media about an individual, personal information made available by third parties on the internet, (e.g., via Google, Facebook, Twitter, etc.).

The reasons here that a journalistic report containing personal information about an individual:

- may contain inaccurate information, allegations, and thus should not (can not) be used as "personal information";
- may be subject to libel and other legal actions by the individual;
- etc.

Further issues pertaining to privacy protection versus journalistic reports on identified individuals resulting in the publishing personal information is a "grey area" which courts in various jurisdictional domains are addressing and thus not yet resolved.

9) This 1st edition does not address the question of negotiated consent but rather considers the simplest case that a learning transaction may be registered which includes a specific form of consent within it.

[13)] A useful example here is found from a health informatics perspective in the ISO standard developed by ISO TC215 "Health Informatics" namely: ISO 22857:2004 titled "*Health informatics – Guidelines on data protection to facilitate trans-border flows of personal health information*.

10) The use of biological characteristics and attributes of an individual which require their physical presence of an individual and are physically "taken" from an individual in a particular context and for a specified role action of an individual. These include the use of biometrics, biological (such as hair, blood, DNA samples), dentistry records, etc.

11) The application of the rights of individuals who are disabled as stated in the "UN Convention on the Rights of Persons with Disabilities" (2006)[14)] Of particular importance here is that this UN Convention takes as its basis the need to support individuals with disabilities to be a fully functioning member of society means that information necessary for these individuals to be able to make commitments including the undertaking of learning transactions shall be made available in a form and format so that the semantics are fully communicated, the individual is able to have informed consent, etc.

12) This 1st edition does not address the role of an "ombudsperson", "Privacy Commissioner", a "Data Protection Commissioner", etc., who serve as an independent adjudicator of complaints, ensure compliance with privacy protection requirements (including of internally of the organization or public administration themselves). Many jurisdictional domains provide for the role of an ombudsperson.

13) Detailed rules pertaining to the use of agents and/or third parties by a LET provider in a learning transaction.

This includes their qualification and assurance of compliance with applicable privacy protection requirements for the personal information pertaining to a learning transaction.

14) An agent acting on behalf of an individual learner

An individual may request an agent to act on its behalf and this may or may not include the individual to require the agent not to reveal the individual identity or any personal information about the individual, i.e., as an anonymous "client" of the agent[15)]

15) detailed rules governing the requirement to tag (or label) at the data elements (or field) level which form part of personal information of an individual generally as was as the business transactions(s) and associated LTIs."

16) Internal behaviour of organizations (and public administration)

Excluded from the scope of this standard is the application of privacy protection requirements within an organization itself. The Open-edi Reference Model, considers these to be internal behaviours of an organization and thus not germane to learning transactions (which focus on external behaviours pertaining to electronic data interchange among the autonomous parties to a learning transaction). As such, excluded from the scope of this standard are any:

a) internal use and management of recorded information pertaining to an identifiable individual by an organization (or public administration) within an organization; and,

b) implementation of internal information management controls, internal procedural controls or operational controls within an organization or public administration necessary for it to comply with applicable privacy requirements that may be required in observance of their lawful or contractual rights, duties and obligations as a legal entity in the jurisdictional domain(s) of which they are part.

[14)] Most, if not all, of the jurisdictional domains of the P-members of ISO/IEC JTC1 are signatories to this UN Convention and are enacting the requirements of this UN Convention into their domestic legislation.

[15)] It may be necessary to introduce and define the concept of an "individual accessibility agent (IAA) as an individual who assists an individual learner from an individual accessibility support perspective, (e.g., someone who "signs", etc.) and thus helps with communication aspects in a neutral (and not tutor) manner. { See further Clause 7.2.3 below}

17) “organizasation Person”

From a public policy privacy protection requirements perspective an “organization Person” is a “natural person” who acts on behalf of and makes commitments of the organization (or public administration) of which that natural person is an “organization part”. But, as an “organization Person, they do not attract inherent rights to privacy.

Examples of roles “organization Person” includes teacher, professor, instructor, tutor, administrator, contractor, consultant, etc., i.e., those working for an organization or public administration.

As such, from a learning transaction perspective, it is an internal behaviour of an organization, as to who makes commitments on behalf of an organization or public administration. How and why organization Persons make decisions and commitments is not germane to the scope and purpose of the 1st edition of this standard. {See further Part 1 of ISO/IEC 15944-1:2010, Clause 6.2 “*Person and external constraints: Individual, organization, and public administration”* as well as its Figure 17 “*Illustration of commitment exchange versus information exchange for organization, organization part(s) and organization Person(s)*”}

18) Specification of aspects related to functional support services (FSV) in an IT-platform neutral manner

19) Interoperability considerations of interfaces among different IT-systems.

It is anticipated that some or all of these requirements will be addressed in future editions of ISO/IEC 29187 or in companion standards or technical reports (including possible new Parts of the multipart ISO/IEC 29187 standard).

1.5 IT-systems environment neutrality

This standard does not assume nor endorse any specific system environment, database management system, database design paradigm, system development methodology, data definition language, command language, system interface, user interface, syntax, computing platform, or any technology required for implementation , i.e., it is information technology neutral. At the same time, this standard maximizes an IT-enabled approach to its implementation and maximizes semantic interoperability.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

They have been divided into two parts; namely:

2.1 ISO/IEC and ISO; and,

2.2 Referenced Specifications.

2.1 ISO/IEC, ISO and ITU[16)]

ISO 639-2:1998 (E/F), *Codes for the representations of names of languages — Part 2: Alpha-3 code/Codes pour la représentation des noms de langue — Partie 2: Code alpha-3.*

ISO 1087-1:2000 (E/F), *Terminology work — Vocabulary — Part 1: Theory and application/Travaux terminologiques — Vocabulaire - Partie 1: Théorie et application.*

ISO/IEC 2382:1976-2011 (E/F), *Information Technology — Vocabulary, Parts 1-36/Technologies de l'information — Vocabulaire, Parties 1-36 (as applicable).*

ISO 3166-1:1997 (E/F), *Codes for the representation of names of countries and their subdivisions — Part 1: Country codes/Codes pour les représentations des noms de pays et de leur subdivisions — Partie 1: Codes pays.*

ISO 3166-2:1998 (E/F), *Codes for the representation of countries and their subdivisions — Part 2: Country subdivision code/Codes pour la représentation des noms de pays et de leurs subdivisions — Partie 2: Code pour les subdivisions de pays.*

ISO 5127:2001 (E), *Information and documentation — Vocabulary.*

ISO/IEC 5218:2004(E/F), *"Information technology — Codes for the Representation of the Human Sexes"/ «Technologies de l'information — Codes de représentation des sexes humains».*

ISO/IEC 6523-1:1998 (E/F), *Information Technology — Structure for the identification of organizations and organization parts Part 1: Identification of organization identification schemes/Technologies de l'information — Structures pour l'identification des organisations et des parties d'organisations — Partie 1: Identification des systèmes d'identification d'organisation.*

ISO/IEC 6523-2:1998 (E/F), *Information Technology — Structure for the identification of organizations and organization parts Part 2: Registration of organizations identification schemes/Technologies de l'information — Structures pour l'identification des organisations et des parties d'organisations — Partie 2: Enregistrement des systèmes d'identification d'organisation.*

---

16) For standards referenced for which both English and French versions are available both the English and French language titles are provided. This is independent of whether the English and French language versions of the standard are published as a single document or as separate documents. For those standards which are available in English only, only the English language title is provided.

Further, the reference to "ISO/IEC" here refers to international standards issued jointly by the ISO and the IEC via its Joint Technical Committee 1 – Information Technology, commonly known as "ISO/IEC JTC1" or just "JTC1". Also, the reference here to the ITU is to those international standards issued by the "ITU-T" (International Telecommunications Union – Telecommunication Standardization sector". and the "ITU-R" (International Telecommunications Union – Radiocommunications Standardization Sector). Note in the field of information and telecommunications technologies, the ITU-T and "ISO/IEC JTC1" often jointly develop and issue international standards.`

ISO/IEC 7501-1:2005(E), *Identification cards — Machine readable travel documents — Part 1: Machine readable passport.*

ISO/IEC 7501-2: 1977(E), *Identification cards — Machine readable travel documents — Part 2: Machine readable visa.*

ISO/IEC 7501-3:2005(E), *Identification cards — Machine readable travel documents — Part 3: Size 1 and Size 2 Machine readable official travel documents.*

ISO/IEC 7812-1:2000(E), *Identification cards — Identification of issuers Part 1: Numbering system.*

ISO/IEC 7812-2: 2000(E), *Identification cards — Identification of issuers — Part 2: Application and registration procedures.*

ISO 8601:2000 (E), *Data elements and interchange formats — Information interchange — Representation of dates and times (available in English only).*

ISO 15489-1:2001 (E/F), *Information and documentation — Records Management Part 1: General / Information et documentation — «records management» — Partie 1: Principes directeurs.*

ISO/IEC 15944-1:2010 (E), *Information Technology — Business Agreement Semantic Descriptive Techniques — Part 1: Operational Aspects of Open-edi for Implementation.*

ISO/IEC 15944-2:2006 (E), *Information Technology — Business Operational View — Part 2: Registration of Scenarios and their Components as Business Objects.*

ISO/IEC 15944-4:2007 (E), *Information technology — Business Operational View — Part 4: Learning transactions and Scenarios – Accounting and Economic Ontology.*

ISO/IEC 15944-5:2008 (E), *Information technology — Business Operational View — Part 5: Identification and referencing of requirements of jurisdictional domains as sources external constraints.*

ISO/IEC 15944-7:2008 (E), *Information technology — Business Operational View — Part 7: eBusiness vocabulary.*

ISO 19108:2000 (E), *Geographic information — Temporal schema*.

ISO 19115:2003 (E), *Geographic information — Metadata*.

ISO/IEC 19501:2005 (E), *Information technology — Open Distributed Processing — Unified Modelling Language (UML)*[17] *Version 1.4.2.*

ISO 22857:2004 (E), *Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health information.*

ISO TS 25237:2008 (E), *Health informatics — Pseudonymization*.

[17] Throughout this document, this standard is simply referenced as “UML”.

2.2 Referenced specifications

APEC Privacy Framework. (2005)

Charter of the United Nations (as signed 1945 and Amended 1965, 1968, and 1973+), United Nation (UN).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) Directive

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980);

UN Convention on the Rights of Disabled Persons (2006+)

Vienna Convention of the Law of Treaties (1969), United Nation (UN)

3 Terms and definitions

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

3.1
address
set of **data elements** that specifies a **location** to which a **recorded information** item(s), a **business** object(s), a material **object**(s) and/or a person(s) can be sent or from which it can be received

NOTE 1 An address can be specified as either a physical address and/or electronic address.

NOTE 2 In the identification, referencing and retrieving of registered business objects, it is necessary to state whether the pertinent recorded information is available in both physical and virtual forms.

NOTE 3 In the context of Open-edi, a “recorded information item” is modelled and registered as an Open-edi scenario (OeS), Information Bundle (IB) or Semantic Component (SC).

[ISO/IEC 15944-2:2006 (3.1)]

3.2
agent (in LET privacy protection)
Person acting for another **Person** in a clearly specified capacity in the context of **a learning transaction**

NOTE 1 Excluded here are agents as "automatons" (or robots, bobots, etc.). In ISO/IEC 14662, "automatons" are recognized and provided for but as part of the Functional Service View (FSV) where they are defined as an "Information Processing Domain (IPD)".

NOTE 2 Adapted from ISO/IEC 15944-1.

3.3
anonymization
process whereby the association between a **set of recorded information (SRI)** and an identifiable **individual** is removed where such an association may have existed

NOTE Adapted from ISO 25237.

[ISO/IEC 15944-8 (3.003)]

3.4
attribute
characteristic of an **object** or **entity**

[ISO/IEC 11179-3:2003 (3.1.3)]

3.5
authentication
provision of assurance of the claimed identity of an **entity**

[ISO/IEC 10181-2:1996 (3.3)]

3.6
authenticity
property that ensures that the identity of a subject or resource is the one claimed

NOTE Authenticity applies to entities such as users, processes, systems and information.

[ISO/IEC TR 13335-1:1996 (3.3)]

3.7
business
series of **processes**, each having a clearly understood purpose, involving more than one **Person**, realized through the exchange of **recorded information** and directed towards some mutually agreed upon goal, extending over a period of time

[ISO/IEC 14662: 2010 (3.2)]

3.8
buyer
Person who aims to get possession of a Good, service and/or right through providing an acceptable equivalent value, usually in money, to the **Person** providing such a Good, service and/or right

[ISO/IEC 15944-1:2011 (3.8)]

3.9
characteristic
abstraction of a **property** of an **object** or of a set of **objects**

NOTE Characteristics are used for describing concepts.

[ISO 1087-1:2000 (3.2.4)]

3.10
character set
finite set of different **characters** that is complete for a given purpose

EXAMPLE The international reference version of the character set of ISO 10646.

[ISO/IEC 2382-4:1999 (04.01.02)]

3.11
classification system (in LET privacy protection)
systematic **identification** and arrangement of learning activities and/or **scenario components** into categories according to logically structured conventions, methods and procedural **rules** as specified in a classification schema

NOTE 1 The classification code or number often serves as a semantic identifier (SI) for which one or more human interface equivalents exist.

NOTE 2 The rules of a classification schema governing the operation of a classification system at times lead to the use of ID codes which have an intelligence built into them, (e.g., in the structure of the ID, the manner in which it can be parsed, etc. Here the use of block-numeric numbering schemas is an often used convention.

NOTE 3 Adapted from ISO/IEC 15944-5.

3.12
code
data representation in different forms according to a pre-established set of **rules**

NOTE In this standard, the "pre-established set of rules" are determined and enacted by a Source Authority and must be explicitly stated.

[ISO 639-2:1998 (3.1)]

3.13
code (in coded domain)
identifier, i.e., an ID **code**, assigned to an **entity** as member of a **coded domain** according to the pre-established set of **rules** governing that **coded domain**

[ISO/IEC 15944-5:2008 (3:19)]

3.14
coded domain
domain for which: (1) the boundaries are defined and explicitly stated as a **rulebase** of a **coded domain Source Authority**; and, (2) each **entity** which qualifies as a member of that domain is identified through the assignment of a unique **ID code** in accordance with the applicable **Registration Schema** of that **Source Authority**

NOTE 1 The rules governing the assignment of an ID code to members of a coded domain reside with its Source Authority and form part of the Coded Domain Registration Schema of the Source Authority.

NOTE 2 Source Authorities which are jurisdictional domains are the primary source of coded domains.

NOTE 3 A coded domain is a data set for which the contents of the data element values are predetermined and defined according to the rulebase of its Source Authority and as such have predefined semantics.

NOTE 4 Associated with a code in a coded domain can be: (a) one and/or more equivalent codes; (b) one and/or more equivalent representations especially those in the form of Human Interface Equivalent (HIE) (linguistic) expressions.

NOTE 5 In a coded domain the rules for assignment and structuring of the ID codes must be specified.

NOTE 6 Where an entity as member of a coded domain is allowed to have, i.e., assigned, more than one ID code, i.e., as equivalent ID codes (possibly including names), one of these must be specified as the pivot ID code.

NOTE 7 A coded domain in turn can consist of two or more coded domains, i.e., through the application of the inheritance principle of object classes.

NOTE 8 A coded domain may contain ID code which pertain to predefined conditions other than qualification of membership of entities in the coded domain. Further, the rules governing a coded domain may or may not provide for user extensions.

EXAMPLE Common examples include: (1) the use of ID Code "0" (or "00", etc.) for “Others, (2) the use of ID Code "9" (or "99", etc.) for “Not Applicable”; (3) the use of “8” (or “98”) for “Not Known”; and/or, if required, (4) the pre-reservation of a series of ID codes for use of “user extensions”.

NOTE 9 In object methodology, entities which are members of a coded domain are referred to as instances of a class.

EXAMPLE In UML modelling notation, an ID code is viewed as an instance of an object class.

[ISO/IEC 15944-2:2006 (3.13)]

3.15
coded Domain Registration Schema (cdRS)
formal **definition** of both (1) the **data** fields contained in the **identification** and specification of an **entity** forming part of the members a **coded domain** including the allowable contents of those fields; and, (2) the **rules** for the assignment of **identifiers**

[ISO/IEC 15944-5:2008 (3.21)]

3.16
coded domain Source Authority (cdSA)
Person, usually an **organization**, as a **Source Authority** which sets the **rules** governing a **coded domain**

NOTE 1 Source Authority is a role of a Person and for widely used coded domains the coded domain Source Authority is often a jurisdictional domain.

NOTE 2 Specific sectors, (e.g., banking, transport, geomatics, agriculture, etc.), may have particular coded domain Source Authority(ies) whose coded domains are used in many other sectors.

NOTE 3 A coded domain Source Authority usually also functions as a Registration Authority but can use an agent, i.e., another Person, to execute the registration function on its behalf.

[ISO/IEC 15944-2:2006 (3.14)]

3.17
collaboration space
business activity space where an economic exchange of valued resources is viewed independently and not from the perspective of any **business** partner

NOTE In collaboration space, an individual partner's view of economic phenomena is de-emphasized. Thus, the common use business and accounting terms like purchase, sale, cash receipt, cash disbursement, raw materials, and finished goods is not allowed because they view resource flows from a participant's perspective.

[ISO/IEC 15944-4:2007 (3.12)]

3.18
commitment
making or accepting of a right, obligation, liability or **responsibility** by a **Person** that is capable of enforcement in the **jurisdictional domain** in which the **commitment** is made

[ISO/IEC 14662:2010 (3.5)]

3.19
composite identifier (in LET privacy protection)
identifier (in a **learning transaction**) functioning as a single unique **identifier** consisting of one or more other **identifiers**, and/or one or more other **data elements**, whose interworking are **rule**-based

NOTE 1 Identifiers (in learning transactions) are for the most part composite identifiers.

NOTE 2 The rules governing the structure and working of a composite identifier should be specified.

NOTE 3 Most widely used composite identifiers consist of the combinations of:

(1) the ID of the overall identification/numbering schema, (e.g., ISO/IEC 6532, ISO/IEC 7812, ISO/IEC 7506, UPC/EAN, ITU-T E.164, etc.), which is often assumed;

(2) the ID of the issuing organization (often based on a block numeric numbering schema); and,

(3) the ID of the entities forming part of members of the coded domain of each issuing organization.

NOTE 4 Adapted from ISO/IEC 15944-8.

3.20
computational integrity
expression of a **standard** in a form that ensures precise description of behaviour and semantics in a manner that allows for automated processing to occur, and the managed evolution of such **standards** in a way that enables dynamic introduction by the next generation of information systems

NOTE Open-edi standards have been designed to be able to support computational integrity requirements especially from a registration and re-use of business objects perspectives.

[ISO/IEC 15944-2:2006 (3.18)]

3.21
constraint (in LET privacy protection)
rule, explicitly stated, that prescribes, limits, governs or specifies any aspect of a **learning transaction**

NOTE 1 Constraints are specified as rules forming part of components of Open-edi scenarios, i.e., as scenario attributes, roles, and/or information bundles.

NOTE 2 For constraints to be registered for implementation in Open-edi, they must have unique and unambiguous identifiers.

NOTE 3 A constraint may be agreed to among parties (condition of contract) and is therefore considered an "internal constraint". Or a constraint may be imposed on parties, (e.g., laws, regulations, etc.), and is therefore considered an "external constraint".

NOTE 4 Adapted from ISO/IEC15944-1.

3.22
consumer
buyer who is an **individual** to whom **consumer protection** requirements are applied as a set of **external constraints** on a **business** transaction

NOTE 1 Consumer protection is a set of explicitly defined rights and obligations applicable as external constraints on a learning transaction.

NOTE 2 The assumption is that a consumer protection applies only where a buyer in a business transaction is an individual. If this is not the case in a particular jurisdiction, such external constraints should be specified as part of scenario components as applicable.

NOTE 3 It is recognized that external constraints on a buyer of the nature of consumer protection may be peculiar to a specified jurisdictional domain.

[ISO/IEC 15944-1:2011 (3.12)]

3.23
consumer protection
set of **external constraints** of a **jurisdictional domain** as rights of a **consumer** and thus as obligations (and possible liabilities) of a **vendor** in a **business** transaction which apply to the good, service and/or right forming the **object** of the **business** transaction (including associated information management and interchange requirements including applicable (sets of) **recorded information**)

NOTE 1 Jurisdictional domains may restrict the application of their consumer protection requirements as applicable only to individuals engaged in a business transaction of a commercial activity undertaken for personal, family or household purposes, i.e., they do not apply to natural persons in their role as "organization" or "organization Person".

NOTE 2 Jurisdictional domains may have particular consumer protection requirements which apply specifically to individuals who are considered to be a "child" or a “minor”, (e.g., those individuals who have not reached their thirteenth (13) birthday).

NOTE 3 Some jurisdictional domains may have consumer protection requirements which are particular to the nature of the good, service and/or right being part of the goal of a learning transaction.

[ISO/IEC 15944-5:2008 (3.33)]

3.24
controlled vocabulary (CV)
vocabulary for which the entries, i.e., **definition/term** pairs, are controlled by a **Source Authority** based on a **rulebase** and **process** for addition/deletion of entries

NOTE 1 In a controlled vocabulary, there is a one-to-one relationship of definition and term.

EXAMPLE The contents of "Clause 3 Definitions" in ISO/IEC standards are examples of controlled vocabularies with the entities being identified and referenced through their ID code, i.e., via their clause numbers.

NOTE 2 In a multilingual controlled vocabulary, the definition/term pairs in the languages used are deemed to be equivalent, i.e., with respect to their semantics.

NOTE 3 The rule base governing a controlled vocabulary may include a predefined concept system.

[ISO/IEC 15944-5:2008 (3.34)]

3.25
data (in a learning transaction)
representations of **recorded information** that are being prepared or have been prepared in a form suitable for use in a computer system

NOTE Adapted from ISO/IEC 15944-1.

3.26
data element
unit of **data** for which the **definition**, **identification**, representation and permissible values are specified by means of a set of **attributes**

[ISO/IEC 11179-1:2004 (3.3.8)]

3.27
data element (in organization of data)
unit of **data** that is considered in context to be indivisible

EXAMPLE The data element "age of a person" with values consisting of all combinations of 3 decimal digits.

NOTE Differs from the entry 17.06.02 in ISO/IEC 2382-17.

[ISO/IEC 2382-4:1999 (04.07.01)]

3.28
dataset
identifiable collection of **data**

NOTE A dataset may be a smaller grouping of data which, though limited by some constraint such as spatial extent or feature type, is located physically within a larger dataset. Theoretically, a dataset may be as small as a single feature or feature attribute contained within a larger dataset. A hardcopy map or chart may be considered a dataset.

[ISO 19115:2003 (4.2)]

3.29
dataset series
collection of **datasets** sharing the same product specification

[ISO 19115:2003 (4.3)]

3.30
data synchronization (in learning transaction)
process of continuous harmonization of a **set(s)** of **recorded information** among all the parties to a **learning transaction** to ensure that the current state of such a **set(s)** of **recorded information** is the same in the **IT systems** of all the participating parties

NOTE 1 Adapted from GS/Global Traceability Standard (GDSN) Glossary.

NOTE 2 Adapted from ISO/IEC 15944-8.

3.31
Decision Making Application (DMA)
model of that part of an **Open-edi system** that makes decisions corresponding to the **role**(s) that the **Open-edi Party** plays as well as the originating, receiving and managing data values contained in the instantiated **Information Bundles** which is not required to be visible to the other **Open-edi Party(ies)**

[ISO/IEC 14662:2010 (3.6)]

3.32
de facto language
natural language used in a **jurisdictional domain** which has the properties and behaviours of **an official language** in that **jurisdictional domain** without having formally been declared as such by that **jurisdictional domain**

NOTE 1 A de facto language of a jurisdictional domain is often established through long term use and custom.

NOTE 2 Unless explicitly stated otherwise and for the purposes of modelling a learning transaction through scenario(s), scenario attributes and/or scenario components, a de facto language of a jurisdictional domain is assumed to have the same properties and behaviours of an official language.

[ISO/IEC 15944-5:2008 (3.42)]

3.33
definition
representation of a concept by a descriptive statement which serves to differentiate it from related concepts

[ISO 1087-1:2000 (3.3.1)]

3.34
designation
representation of a concept by a sign which denotes it

NOTE In terminology work three types of designations are distinguished: symbols, appellations, (a.k.a. names), and terms.

[ISO 1087-1:2000 (3.4.1)]

3.35
distinguishing identifier
data that unambiguously distinguishes an **entity** in the **authentication process**

[ISO/IEC 10181-2:1996 (3.11)]

3.36
eBusiness (in learning transaction)
learning transaction, involving the making of **commitments**, in a defined **collaboration space**, among **Persons** using their **IT systems**, according to **Open-edi standards**

NOTE 1 eBusiness can be conducted on both a for-profit and not-for-profit basis.

NOTE 2 A key distinguishing aspect of eBusiness is that it involves the making of commitment(s) of any kind among the Persons in support of a mutually agreed upon goal, involving their IT systems, and doing so through the use of EDI (using a variety of communication networks including the Internet).

NOTE 3 eBusiness includes various application areas such as “e-commerce”, “e-administration”, “e-logistics”, “e-government”, “e-medicine”, “e-learning”, etc.

NOTE 4 The equivalent French language term for “eBusiness” is always presented in its plural form.

NOTE 5 Adapted from ISO/IEC 15944-7.

3.37
electronic address
address used in a recognized electronic addressing scheme, (e.g., telephone, telex, IP, etc.), to which **recorded information** item(s) and/or business object(s) can be sent to or received from a Contact

[ISO/IEC 15944-2:2006 (3.32)]

3.38
Electronic Data Interchange (EDI)
automated exchange of any predefined and structured **data** for **business** purposes among information systems of two or more **Persons**

NOTE This definition includes all categories of electronic learning transactions.

[ISO/IEC 14662:2004 (3.8)]

3.39
entity
any concrete or abstract thing that exists, did exist, or might exist, including associations among these things

EXAMPLE A person, object, event, idea, process, etc.

NOTE An entity exists whether data about it are available or not.

[ISO/IEC 2382-17:1999 (17.02.05)]

3.40
entity authentication
corroboration that the **entity** is the one claimed

[ISO/IEC 9788-1:1997 (3.3.1)]

3.41
exchange code set
set of **ID codes** identified in **a coded domain** as being suitable for information exchange as shareable **data**

EXAMPLE The 3 numeric, 2-alpha and 3-alpha code sets in ISO 3166-1.

[ISO/IEC 15944-5:2008 (3.49)]

3.42
external constraint (in LET privacy protection)
constraint which takes precedence over **internal constraints** in a **learning transaction**, i.e., is external to those agreed upon by the parties to a **learning transaction**

NOTE 1 Normally external constraints are created by law, regulation, orders, treaties, conventions or similar instruments.

NOTE 2 Other sources of external constraints are those of a sectoral nature, those which pertain to a particular jurisdictional domain or a mutually agreed to common business conventions, (e.g., INCOTERMS, exchanges, etc.).

NOTE 3 External constraints can apply to the nature of the good, service and/or right provided in a learning transaction.

NOTE 4 External constraints can demand that a party to a learning transaction meet specific requirements of a particular role.

EXAMPLE 1 Only a qualified medical doctor may issue a prescription for a controlled drug.

EXAMPLE 2 Only an accredited share dealer may place transactions on the New York Stock Exchange.

EXAMPLE 3 Hazardous wastes may only be conveyed by a licensed enterprise.

NOTE 5 Where the information bundles (IBs), including their Semantic Components (SCs) of a learning transaction are also to form the whole of a learning transaction, (e.g., for legal or audit purposes), all constraints must be recorded.

EXAMPLE There may be a legal or audit requirement to maintain the complete set of recorded information pertaining to a learning transaction, i.e., as the information bundles exchanged, as a "record".

NOTE 6 EXAMPLE A minimum external constraint applicable to a learning transaction often requires one to differentiate whether the Person, i.e., that is a party to a learning transaction, is an "individual", "organization", or "public administration". For example, privacy rights apply only to a Person as an "individual".

NOTE 7 Adapted from ISO/IEC 15944-1.

3.43
Formal Description Technique (FDT)
specification method based on a description language using rigorous and **unambiguous rules** both with respect to developing expressions in the language (formal syntax) and interpreting the meaning of these expressions (formal semantics)

[ISO/IEC 14662:2010 (3.9)]

3.44
Functional Service View (FSV)
perspective of **business** transactions limited to those information technology interoperability aspects of **IT Systems** needed to support the execution of **Open-edi** transactions

[ISO/IEC 14662:2010 (3.10)]

3.45
Human Interface Equivalent (HIE)
representation of the **unambiguous** and IT-enabled semantics of an **IT interface equivalent**, often the **ID code** of a **coded domain** (or a **composite identifier**), in a formalized manner suitable for communication to and understanding by humans

NOTE 1 Human interface equivalents can be linguistic or non-linguistic in nature but their semantics remains the same although their representations may vary.

NOTE 2 In most cases there will be multiple Human Interface Equivalent representations as required to meet localization requirements, i.e. those of a linguistic nature, jurisdictional nature, and/or sectoral nature.

NOTE 3 Human Interface Equivalents include representations in various forms or formats, (e.g., in addition to written text those of an audio, symbol (and icon) nature, glyphs, image, etc.).

[ISO/IEC 15944-2:2006 (3.35)]

3.46
IB Identifier
unique, linguistically neutral, **unambiguous** referenceable **identifier** for an **Information Bundle**

[ISO/IEC 15944-2:2006 (3.36)]

3.47
ID Code
identifier assigned by the **coded domain Source Authority (cdSA)** to a member of a **coded domain ID**

NOTE 1 ID codes must be unique within the Registration Schema of that coded domain.

NOTE 2 Associated with an ID code in a coded domain can be: (a) one or more equivalent codes; (b) one or more equivalent representations, especially those in the form of human equivalent (linguistic) expressions.

NOTE 3 Where an entity as a member of a coded domain is allowed to have more than one ID code, i.e., as equivalent codes (possibly including names), one of these must be specified as the pivot ID code.

NOTE 4 A coded domain may contain ID codes pertaining to entities which are not members as peer entities, i.e., have the same properties and behaviours, such as ID codes which pertain to predefined conditions other than member entities. If this is the case, the rules governing such exceptions must be predefined and explicitly stated.

EXAMPLE Common examples include: (1) the use of an ID code "0" (or "00", etc.), for “Other”; (2) the use of an ID code "9" (or "99") for “Not Applicable”; (3) the use of “8” (or “98”) for “Not Known”; if required, (4) the pre-reservation of a series or set of ID codes for use for "user extensions".

NOTE 5 In UML modeling notation, an ID code is viewed as an instance of an object class.

[ISO/IEC 15944-2:2006 (3.37)]

3.48
identification
rule-based **process**, explicitly stated, involving the use of one or more **attributes**, i.e., **data elements**, whose value (or combination of values) are used to identify uniquely the occurrence or existence of a specified **entity**

[ISO/IEC 15944-1:2011 (3.26)]

3.49
identifier (in learning transaction)
unambiguous, unique and a linguistically neutral value, resulting from the application of a **rule**-based **identification process**

NOTE 1 Identifiers must be unique within the identification scheme of the issuing authority.

NOTE 2 An identifier is a linguistically independent sequence of characters capable of uniquely and permanently identifying that with which it is associated. {See ISO 19135:2005 (4.1.5)}

NOTE 3 Adapted from ISO/IEC 15944-1.

3.50
individual
Person who is a human being, i.e., a natural person, who acts as a distinct indivisible **entity** or is considered as such

[ISO/IEC 15944-1:20011 (3.28)]

3.51
individual accessibility (in LET privacy protection)
set of **external constraints** of a **jurisdictional domain** as rights of an **individual** with disabilities to be able to use IT systems at the human, i.e., user, interface and the concomitant obligation of a **LET provider** to provide such adaptive technologies

NOTE 1 Although “accessibility” typically addresses users who have a disability, the concept is not limited to disability issues.

EXAMPLE Examples of disabilities in the form of functional and cognitive limitations include:

— people who are blind;

— people with low vision;

— people with colour blindness;

— people who are hard of hearing or deaf, i.e., are hearing impaired;

— people with physical disabilities;

— people with language or cognitive disabilities.

NOTE 2 Adapted from ISO/IEC 15944-5.

3.52
individual anonymity
state of not knowing the identity or no having any recording of **personal information** on or about an **individual** as a learner by the **LET provider** or **regulator**, (or any other party) to a **learning transaction**

NOTE Adapted from ISO/IEC 15944-8.

3.53
individual authentication (in LET privacy protection)
provision of the assurance of a **recognized individual identity (rii)** sufficient for the purpose of the **learning transaction**

NOTE Adapted from ISO/IEC 15944-8.

3.54
individual identity (ii) (in LET privacy protection)
Person identity of an **individual**, i.e., an individual identity, consisting of the combination of the **persona** information and **identifier** used by an **individual** in a **learning transaction**, i.e., the making of any kind of **commitment**

NOTE Adapted from ISO/IEC 15944-8.

3.55
individual learner
learner who participates as an **individual** in a **learning transaction**

3.56
individual persona Registration Schema (ipRS)
persona Registration Schema (pRS) where the **persona** is, or includes, that of an **individual** being registered

NOTE 1 Where an persona Registration Schema includes persona of sub-types of Persons, i.e., individuals, organizations, and/or, public administrations, those which pertain to individuals shall be identified as such because public policy as external constraints apply including those of a privacy protection requirements nature.

NOTE 2 In a individual persona Registration Schema, one shall state whether or not a truncated name, i.e. registered persona, of the individual, is allowed or mandatory, and if so the ipRS shall explicitly state the rules governing the formation of the same.

[ISO/IEC 15944-8 (3.060)]

3.57
Information Bundle (IB)
formal description of the semantics of the **recorded information** to be exchanged by **Open-edi Parties** playing roles in an **Open-edi scenario**

[ISO/IEC 14662:2010 (3.11)]

3.58
information law
any law, regulation, policy, or code (or any part thereof) that requires the creation, receipt, collection, description or listing, production, retrieval, submission, retention, storage, preservation or destruction of **recorded information**, and/or that places conditions on the access and use, confidentiality, privacy, integrity, accountabilities, continuity and availability of the processing, reproduction, distribution, transmission, sale, sharing or other handling of **recorded information**

[ISO/IEC 15944-8 (3.062)]

3.59
Information Processing Domain (IPD)
Information Technology System which includes at least either a **Decision Making Application** (DMA) and/or one of the components of an Open-edi Support Infrastructure (or both), and acts/executes on behalf of an **Open-edi Party** (either directly or under a delegated authority)

[ISO/IEC 14662:2010 (3.12)]

3.60
Information Technology System (IT System)
set of one or more computers, associated software, peripherals, terminals, human operations, physical **processes**, information transfer means, that form an autonomous whole, capable of performing information processing and/or information transfer

[ISO/IEC 14662:2010 (3.13)]

3.61
internal constraint (in LET privacy protection)
constraint which forms part of the **commitment**(s) mutually agreed to among the parties to a **learning transaction**

NOTE 1 Internal constraints are self-imposed. They provide a simplified view for modelling and re-use of scenario components of a learning transaction for which there are no external constraints or restrictions to the nature of the conduct of a learning transaction other than those mutually agreed to by the individual learner and LET provider.

NOTE 2 Adapted from ISO/IEC 15944-1.

3.62
IT-enablement (in LET privacy protection)
transformation of a current **standard** used in **learning transactions**, (e.g., **coded domains**), from a manual to computational perspective so as to be able to support **commitment** exchange and **computational integrity**

NOTE Adapted from ISO/IEC 15944-8.

3.63
jurisdictional domain (in LET privacy protection)
jurisdiction, recognized in law as a distinct legal and/or regulatory framework, which is a source of **external constraints** on **Persons**, their behaviour and the making of **commitments** among **Persons** including any aspect of a **learning transaction**

NOTE 1 The pivot jurisdictional domain is a United Nations (UN) recognized member state. From a legal and sovereignty perspective they are considered "peer" entities. Each UN member state, (a.k.a. country) may have sub-administrative divisions as recognized jurisdictional domains, (e.g., provinces, territories, cantons, länder, etc.), as decided by that UN member state.

NOTE 2 Jurisdictional domains can combine to form new jurisdictional domains, (e.g., through bilateral, multilateral and/or international treaties).

EXAMPLE Included here, for example, are the European Union (EU), NAFTA, WTO, WCO, ICAO, WHO, Red Cross, the ISO, the IEC, the ITU, etc.

NOTE 3 Several levels and categories of jurisdictional domains may exist within a jurisdictional domain.

NOTE 4 A jurisdictional domain may impact aspects of the commitment(s) made as part of a learning transaction including those pertaining to the making, selling, transfer of goods, services and/or rights (and resulting liabilities) and associated information. This is independent of whether such interchange of commitments are conducted on a for-profit or not-for-profit basis and/or include monetary values.

NOTE 5 Laws, regulations, directives, etc., issued by a jurisdictional domain are considered as parts of that jurisdictional domain and are the primary sources of external constraints on learning transactions.

NOTE 6 Adapted from ISO/IEC 15944-5.

3.64
jurisdictional domain identifier
ID code of a **jurisdictional domain** as recognized for use by peer **jurisdictional domains** within a system of mutual recognition

[ISO/IEC 15944-2:2006 (3.47)]

3.65
language
system of signs for communication, usually consisting of a **vocabulary** and **rules**

NOTE In this part of ISO/IEC 21987, language refers to natural languages or special languages, but not "programming languages" or "artificial languages".

[ISO 5127-1:2001 (1.1.2.01)]

3.66
language code
combination of **characters** used to represent a **language** or **languages**

NOTE In ISO/IEC 29187, the ISO 639-2/T (terminology) three alpha-codes, shall be used.

[ISO 639-2:1998 (3.2)]

3.67
learning collaboration space
learning activity space where exchanges of **recorded information**, valued resources, and related activities is viewed independently and not from the perspective of any party to a **learning transaction**

NOTE Adapted from ISO/IEC 15944-4.

3.68
learning event
occurrence in time that partners to a **learning transaction** wish to monitor or control

NOTE 1 Learning events are the workflow tasks that learning partners need to accomplish to complete a learning transaction among themselves. As learning events occur, they cause a learning transaction to move through its various phases of planning, identification, negotiation, actualization, and post-actualization.

NOTE 2 Occurrences in time can either be: (1) internal as mutually agreed to among the parties to a learning transaction; and/or, (2) reference some common publicly available and recognized date/time referencing schema, (e.g., one based on using the ISO 8601 and/or ISO 19135 standards).

NOTE 3 Adapted from ISO/IEC 15944-4.

3.69
learning object
unambiguously identified, specified, referenceable, registered and re-useable **Open-edi scenario** or **scenario component** of a **learning transaction**

NOTE 1 As an “object”, a “learning object” exists only in the context of a learning transaction.

NOTE 2 Adapted from ISO/IEC 15944-2.

3.70
learning transaction
predefined set of activities and/or **processes** among **Persons** which is initiated by a **Person** to accomplish an explicitly stated learning goal and terminated upon recognition of one of the agreed conclusions by all the involved **Persons** although some of the recognition may be implicit

NOTE 1 A learning transaction may be internal constraints-based or external constraints-based. A primary example of an external constraint-based learning transaction is that of jurisdictional domains governing minimum levels of schooling, (e.g., K-12).

NOTE 2 A learning transaction can be on a for-a-fee or for-free basis.

NOTE 3 A LET provider can offer a learning transaction and operate on either a for-profit or not-for-profit basis.

NOTE 4 Adapted from ISO/IEC 14662.

3.71
learning transaction identifier (LTI)
identifier assigned by a **LET provider** or a **regulator** to an instantiated **learning transaction** among the **Persons** involved

NOTE 1 The identifier assigned by the LET provider or regulator shall have the properties and behaviours of an “identifier (in a learning transaction)”.

NOTE 2 As an identifier (in a learning transaction), a LTI serves as the unique common identifier for all Persons involved for the identification, referencing, retrieval of recorded information, etc., pertaining to the commitments made and the resulting actualization (and post-actualization) of the learning transaction agreed to.

NOTE 3 A learning transaction identifier can be assigned at any time during the planning, identification or negotiation phases but shall be assigned at least prior to the start or during the actualization phase.

NOTE 4 As and where required by the applicable jurisdictional domain(s), the recorded information associated with the learning transaction identifier (LTI) may well require the LET provider to include other identifiers, (e.g., from a value-added good or service tax, etc., perspective) as assigned by the applicable jurisdictional domain(s).

NOTE 5 Adapted from ISO/IEC 15944-5.

3.72
legally recognized individual identity (LRII)
recognized individual identity (rii) which includes the use of a **recognized individual name (RIN)** and the associated **identifier**, i.e., **ID code**, assigned as part of the **personal information** for that **individual** in the **individual persona Registration Schema (ipRS)**

3.73
legally recognized individual persona Registration Schema (LipRS)
individual persona Registration Schema (ipRS) which has legal status and is so recognized in a **jurisdictional domain** as being able to register a **recognized individual name (RIN)** and unique **identifier** associated with such a registration

3.74
legally recognized language (LRL)
natural language which has status (other than an **official language** or **de facto language**) in a **jurisdictional domain** as stated in an act, regulation, or other legal instrument, which grants a community of people (or its **individuals**) the right to use that **natural language** in the context stipulated by the legal instrument(s)

NOTE The LRL can be specified through either: (a) the identification of a language by the name used; or, (b) the identification of a people and thus their language(s).

EXAMPLE In addition to acts and regulations, legal instruments include self-government agreements, land claim settlements, court decisions, jurisprudence, etc.

[ISO/IEC 15944-5:2008 (3.71)]

3.75
legally recognized name (LRN)
persona associated with a **role** of a **Person** recognized as having legal status and so recognized in a **jurisdictional domain** as accepted or assigned in compliance with the **rules** applicable of that **jurisdictional domain**, i.e. as governing the **coded domain** of which the **LRN** is a member

NOTE 1 A LRN may be of a general nature and thus be available for general use in commitment exchange or may arise from the application of a particular law, regulation, program or service of a jurisdictional domain and thus will have a specified use in commitment exchange.

NOTE 2 The process of establishment of a LRN is usually accompanied by the assignment of a unique identifier.

NOTE 3 A LRN is usually a registry entry in a register established by the jurisdictional domain (usually by a specified public administration within that jurisdictional domain) for the purpose of applying the applicable rules and registering and recording LRNs (and possible accompanying unique identifiers accordingly).

NOTE 4 A Person may have more than one LRN (and associated LRN identifier).

[ISO/IEC 15944-5:2008 (3.72)]

3.76
LET Functional Services Support View (LET-FSV)
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.

3.77
LET- Operational View (LET-OV)
perspective of **learning transactions** limited to those aspects regarding the making of **learning** decisions and **commitments** among **Persons**, which are needed for the description of a **learning transaction**

NOTE Adapted from ISO/IEC 14662.

3.78
LET privacy collaboration space (PCS)
modelling or inclusion of an **Open-edi scenario** of a **collaboration space** involving an **individual** as the learner in a potential or actualized **learning transaction** where the learner is an **individual** and therefore **privacy protection** requirements apply to **personal information** of that **individual**

NOTE Adapted from ISO/IEC 15944-8.

3.79
LET provider
Person, as **organization** or **public administration** which provides a good, service, and/or right in the fields of learning, education or training as part of a **learning transaction**

3.80
list
ordered **set** of **data elements**

[ISO/IEC 2382-4:1999 (04.08.01)]

3.81
localization
pertaining to or concerned with anything that is not global and is bound through specified sets of **constraints** of:

a) a linguistic nature including **natural** and **special languages** and associated multilingual requirements;

b) jurisdictional nature, i.e., legal, regulatory, geopolitical, etc.;

c) a sectoral nature, i.e., industry sector, scientific, professional, etc.;

d) a human rights nature, i.e., privacy, disabled/handicapped persons, etc.;

e) consumer behaviour requirements; and/or,

f) safety or health requirements.

Within and among "locales", interoperability and harmonization objectives also apply

[ISO/IEC 15944-5:2008 (3.75)]

3.82
location
place, either physical or electronic, that can be defined as an **address**

[ISO/IEC 15944-2:2006 (3.50)]

3.83
medium
physical material which serves as a functional unit, in or on which information or **data** is normally recorded, in which information or **data** can be retained and carried, from which information or **data** can be retrieved, and which is non-volatile in nature

NOTE 1 This definition is independent of the material nature on which the information is recorded and/or technology used to record the information, (e.g., paper, photographic, (chemical), magnetic, optical, ICs (integrated circuits), as well as other categories no longer in common use such as vellum, parchment (and other animal skins), plastics, (e.g., bakelite or vinyl), textiles, (e.g., linen, canvas), metals, etc.).

NOTE 2 The inclusion of the "non-volatile in nature" attribute is to cover latency and records retention requirements.

NOTE 3 This definition of "medium" is independent of: i) form or format of recorded information; ii) physical dimension and/or size; and, iii) any container or housing that is physically separate from material being housed and without which the medium can remain a functional unit.

NOTE 4 This definition of "medium" also captures and integrates the following key properties: i) the property of medium as a material in or on which information or data can be recorded and retrieved; ii) the property of storage; iii) the property of physical carrier; iv) the property of physical manifestation, i.e., material; v) the property of a functional unit; and, vi) the property of (some degree of) stability of the material in or on which the information or data is recorded.

[ISO/IEC 15944-1:2011 (3.34)]

3.84
model
abstraction of some aspect of reality

[ISO 19115:2003 (4.9)]

3.85
multilingualism
ability to support not only **character sets** specific to a (natural) **language** (or family of **languages**) and associated **rules** but also **localization** requirements, i.e., use of a **language** from **jurisdictional domain**, sectoral and/or **consumer** marketplace perspectives

[ISO/IEC 15944-5:2008 (3.82)]

3.86
mutually defined – recognized individual identity (md-rii) (in LET privacy protection)
recognized individual identity (rii) which is mutually defined and agreed to for use between the **LET provider** and the **individual**, as learner, in a **learning transaction**

NOTE 1 The establishment of a mutually agreed to and recognized individual between a seller and individual, as buyer, does not extinguish the applicable privacy protection rights of that individual.

NOTE 2 A mutually defined recognized individual identity (md-rii) shall be established between the seller and the individual no later than the end of the negotiation phase.

NOTE 3 Use of a mutually defined recognized individual identity (md-rii) may not be permitted where external constraints apply.

NOTE 4 Adapted from ISO/IEC 15944-8.

3.87
name
designation of an **object** by a linguistic expression

[ISO 5217:2000 (1.1.2.13)]

3.88
natural language
language which is or was in active use in a community of people, and the **rules** of which are mainly deduced from the usage

[ISO 5217:2000 (1.1.2.02)]

3.89
object
anything perceivable or conceivable

NOTE Objects may be material, (e.g., engine, a sheet of paper, a diamond), or immaterial, (e.g., conversion ratio, a project play) or imagined, (e.g., a unicorn).

[ISO 1087-1:2000 (3.1.1)]

3.90
object class
set of ideas, abstractions, or things in the real world that can be identified with explicit boundaries and meaning and whose properties and behavior follow the same **rules**

[ISO/IEC 11179-1:2004 (3.3.22)]

3.91
official language
external constraint in the form of a **natural language** specified by a **jurisdictional domain** for official use by **Persons** forming part of and/or subject to that **jurisdictional domain** for use in communication(s) either

1) within that **jurisdictional domain**; and/or,

2) among such **Persons**, where such communications are **recorded information** involving **commitment**(s)

NOTE 1 Unless official language requirements state otherwise, Persons are free to choose their mutually acceptable natural language and/or special language for communications as well as exchange of commitments.

NOTE 2 A jurisdictional domain decides whether or not it has an official language. If not, it will have a de facto language.

NOTE 3 An official language(s) can be mandated for formal communications as well as provision of goods and services to Persons subject to that jurisdictional domain and for use in the legal and other conflict resolution system(s) of that jurisdictional domain, etc.

NOTE 4 Where applicable, use of an official language may be required in the exercise of rights and obligations of individuals in that jurisdictional domain.

NOTE 5 Where an official language of a jurisdictional domain has a controlled vocabulary of the nature of a terminology, it may well have the characteristics of a special language. In such cases, the terminology to be used must be specified.

NOTE 6 For an official language, the writing system(s) to be used shall be specified, where the spoken use of a natural language has more than one writing system.

EXAMPLE 1 The spoken language of use of an official language may at times have more than one writing system. For example, three writing systems exist for the Inuktitut language. Canada uses two of these writing systems, namely, a Latin-1 based (Roman), the other is syllabic-based. The third is used in Russia and is Cyrillic based.

EXAMPLE 2 Another example is that of Norway which has two official writing systems, both Latin-1 based, namely, Bokmål (Dano-Norwegian) and Nynorsk (New Norwegian).

NOTE 7 A jurisdictional domain may have more than one official language but these may or may not have equal status.

EXAMPLE Canada has two official languages; Switzerland has three, while the Union of South Africa has eleven official languages.

NOTE 8 The BOV requirement of the use of a specified language will place that requirement on any FSV supporting service.

EXAMPLE A BOV requirement of Arabic, Chinese, Russian, Japanese, Korean, etc., as an official language requires the FSV support service to be able to handle the associated character sets.

[ISO/IEC 15944-5:2008 (3.87)]

3.92
Open-edi
electronic data interchange among multiple autonomous **Persons** to accomplish an explicitly shared **business** goal according to **Open-edi standards**

[ISO/IEC 14662:2010 (3.14)]

3.93
Open-edi Description Technique (OeDT)
specification method such as a **Formal Description Technique**, another methodology having the **characteristics** of a **Formal Description Technique**, or a combination of such techniques as needed to formally specify **BOV** concepts, in a computer processable form

[ISO/IEC 14662:2010 (3.16)]

3.94
Open-edi disposition
process governing the implementation of formally approved records retention, destruction (or expungement) or transfer of **recorded information** under the control of a **Person** which are documented in disposition authorities or similar instruments

NOTE Adapted from ISO 15489-1.

[ISO/IEC 15944-5:2008 (3.90)]

3.95
Open-edi Party (OeP)
Person that participates in **Open-edi**

NOTE Often referred to generically in this, and other eBusiness standards, (e.g., parts of the ISO/IEC 15944 multipart "eBusiness" standard) as "party" or "parties" for any entity modelled as a Person as playing a role in Open-edi scenarios.

[ISO/IEC 14662:2010 (3.17)]

3.96
Open-edi Record Retention (OeRR) (in LET privacy protection)
specification of a period of time that a **set of recorded information** must be kept by a **Person** in order to meet operational, legal, regulatory, fiscal or other requirements as specified in the **external constraints** (or **internal constraints**) applicable to a **Person** who is a party to a **learning transaction**

NOTE Adapted from ISO/IEC 15944-5.

3.97
Open-edi system
information technology system (IT system) which enables an **Open-edi Party** to participate in Open-edi transactions

[ISO/IEC 14662:2010 (3.22)]

3.98
organization
unique framework of authority within which a person or persons act, or are designated to act, towards some purpose

NOTE The kinds of organizations covered by this International Standard include the following examples:

EXAMPLE 1 An organization incorporated under law.

EXAMPLE 2 An unincorporated organization or activity providing goods and/or services including:

1) partnerships;

2) social or other non-profit organizations or similar bodies in which ownership or control is vested in a group of individuals;

3) sole proprietorships

4) governmental bodies.

EXAMPLE 3 Groupings of the above types of organizations where there is a need to identify these in information interchange.

[ISO/IEC 6523-1:1998 (3.1)]

3.99
organization part
any department, service or other **entity** within an **organization**, which needs to be identified for information interchange

[ISO/IEC 6523-1:1998 (3.2)]

3.100
organization Person
organization part which has the properties of a **Person** and thus is able to make **commitments** on behalf of that **organization**

NOTE 1 An organization can have one or more organization Persons.

NOTE 2 An organization Person is deemed to represent and act on behalf of the organization and to do so in a specified capacity.

NOTE 3 An organization Person can be a "natural person" such as an employee or officer of the organization.

NOTE 4 An organization Person can be a legal person, i.e., another organization.

[ISO/IEC 15944-1:2011 (3.46)]

3.101
Person
entity, i.e., a natural or legal person, recognized by law as having legal rights and duties, able to make **commitment**(s), assume and fulfill resulting obligation(s), and able of being held accountable for its action(s)

NOTE 1 Synonyms for "legal person" include "artificial person", "body corporate", etc., depending on the terminology used in competent jurisdictions.

NOTE 2 "Person" is capitalized to indicate that it is being used as formally defined in the standards and to differentiate it from its day-to-day use.

NOTE 3 Minimum and common external constraints applicable to a learning transaction often require one to differentiate among three common subtypes of Person, namely "individual", "organization", and "public administration".

[ISO/IEC 14662:2010 (3.24)]

3.102
persona
set of **data elements** and their values by which a **Person** wishes to be known and thus identified in a **learning transaction**

NOTE Adapted from ISO/IEC 15944-1.

3.103
personal information
any information about an identifiable **individual** that is recorded in any form, including electronically or on paper

NOTE Some examples would be record information about a person's religion, age, financial transactions, medical history, address, or blood type.

[ISO/IEC 15944-5:2008 (3.103)]

3.104
persona Registration Schema (pRS)
formal **definition** of the **data** fields contained in the specification of a **persona** of a **Person** and the allowable contents of those fields, including the **rules** for the assignment of **identifiers**. (This may also be referred to as a "**persona** profile" of a **Person**)

[ISO/IEC 15944-1:2011 (3.52)]

3.105
Person authentication
provision of the assurance of a **recognized Person identity (rPi)** (sufficient for the purpose of the **learning transaction**) by corroboration

NOTE Adapted from ISO/IEC 15944-1.

3.106
Person identity (Pi) (in LET privacy protection)
combination of **persona information** and **identifier** used by a **Person** in a **learning transaction**

NOTE Adapted from ISO/IEC 15944-1.

3.107
Person signature
signature, i.e., a **name** representation, distinguishing mark or usual mark, which is created by and pertains to a **Person**

[ISO/IEC 15944-1:2011 (3.50)]

3.108
personal information filing system
any structured set of **personal information** which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis

[ISO/IEC 15944-8 (3.102)]

3.109
physical address
address that is used/recognized by a postal authority and/or courier service to deliver information item(s), material **object**(s), or **business object**(s) to a Contact at either an actual **address** or a pick-up point **address**, (e.g., P.O. Box, rural route, etc.)

[ISO/IEC 15944-2:2006 (3.80)]

3.110
pivot code set
set of **ID codes** in a **coded domain** which is made publicly known and available, the most stable, representing the defined semantics. (Most often it is the same as the **ID code**)

NOTE 1 The use of the pivot code set (as per Part 5) as distinguished from the ID code supports the requirement of a Source Authority to maintain internally and on a confidential basis the ID code of its members.

NOTE 2 At times a coded domain has more than one valid code set, (e.g., ISO 639, ISO 3166, etc.)

EXAMPLE In ISO 3166-1 the 3-digit numeric code is the pivot. The 2-alpha and 3-alpha code sets can change when the name of the entity referenced is changed by that entity.

[ISO/IEC 15944-5:2008 (3.104)]

3.111
pivot ID code
most stable **ID code** assigned to identify a member of a **coded domain** where more than one **ID code** may be assigned and/or associated with a member of that **coded domain**

EXAMPLE ISO 3166-1:1997 (E/F) "Codes for the representation of names of countries and their subdivisions – Part 1: Country codes/Codes pour la représentations des noms de pays et de leur subdivisions – Partie 1: Codes pays" contains three code sets: (a) a three digit numeric code; (b) a two alpha code; (c) a three alpha code.

In this case, the three digit numeric code serves as the pivot code. It is the most stable, remains the same even though the two alpha and/or three alpha codes may and do change.

[ISO/IEC 15944-5:2008 (3.105)]

3.112
principle
fundamental, primary assumption and quality which constitutes a source of action determining particular objectives or results

NOTE 1 A principle is usually enforced by rules that affect its boundaries.

NOTE 2 A principle is usually supported through one or more rules.

NOTE 3 A principle is usually part of a set of principles which together form a unified whole.

EXAMPLE Within a jurisdictional domain, examples of a set of principles include a charter, a constitution, etc.

[ISO/IEC 15944-2:2006 (3.81)]

3.113
privacy protection (in LET privacy protection)
set of **external constraints** of a **jurisdictional domain** pertaining to **recorded information** on or about an identifiable **individual**, i.e., **personal information**, with respect to the creation, collection, management, retention, access and use and/or distribution of such **recorded information** about that **individual** including its accuracy, timeliness, and relevancy

NOTE 1 Recorded information collected or created for a specific purpose on an identifiable individual, i.e., the explicitly shared goal of the learning transaction involving an individual shall not be used for another purpose without the explicit and informed consent of the individual to whom the recorded information pertains.

NOTE 2 Privacy requirements include the right of an individual to be able to view the recorded information about him/her and to request corrections to the same in order to ensure that such recorded information is accurate and up-to-date.

NOTE 3 Where jurisdictional domains have legal requirements which override privacy protection requirements these must be specified, (e.g., national security, investigations by law enforcement agencies, etc.).

NOTE 4 Adapted from ISO/IEC 15944-8.

[ISO/IEC 15944-5:2008 (3.109)]

3.114
privacy protection officer (PPO)
organization Person authorized by the **organization** to act on behalf of that **organization** and entrusted by the **organization** as the officer responsible for the overall governance and implementation of the privacy protection requirements for information life cycle management not only within that **organization** but also with respect to any **electronic data interchange** of **personal information** on the **individual** concerned with parties to the **learning transaction**, including a regulator where required, as well as any **agents**, **third parties** involved in that **learning transaction**

NOTE Adapted from ISO/IEC 15944-8.

3.115
process
series of actions or events taking place in a defined manner leading to the accomplishment of an expected result

[ISO/IEC 15944-1:2011 (3.53)]

3.116
processing of personal information
any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction

[ISO/IEC 15944-8:2010-06-23 (3.111)]

3.117
property
peculiarity common to all members of an **object class**

[ISO/IEC 11179-1:2004 (3.3.29)]

3.118
pseudonym
use of a **persona** or other **identifier** by an **individual** which is different from that used by the **individual** with the intention that it be not linkable to that **individual**

NOTE Adapted from ISO TS 25237.

3.119
pseudonymization
particular type of anonymization that removes the associate with an **individual** and adds an associate between a particular set of **characteristics** relating to the **individual** and one more **pseudonym**

NOTE Adapted from ISO TS 25237.

[ISO/IEC 15944-8 (3.114)]

3.120
public administration
entity, i.e., a **Person**, which is an **organization** and has the added **attribute** of being authorized to act on behalf of a **regulator**

[ISO/IEC 15944-1:2011 (3.54)]

3.121
public policy
category of **external constraints** of a **jurisdictional domain** specified in the form of a right of an **individual** or a requirement of an **organization** and/or **public administration** with respect to an **individual** pertaining to any exchange of **commitments** among the parties concerned involving a good, service and/or right including information management and interchange requirements

NOTE 1 Public policy requirements may apply to any one, all or combinations of the fundamental activities comprising a learning transaction, i.e., planning, identification, negotiation, actualization and post-actualization. {See further Clause 6.3 "Rules governing the process component" in ISO/IEC 15944-1:2002}

NOTE 2 It is up to each jurisdictional domain to determine whether or not the age of an individual qualifies a public policy requirement, (e.g., those which specifically apply to an individual under the age of thirteen (13) as a "child", those which require an individual to have attained the age of adulthood, (e.g., 18 years or 21 years of age) of an individual to be able to make commitments of a certain nature.

NOTE 3 Jurisdictional domains may have consumer protection or privacy requirements which apply specifically to individuals who are considered to be "children", "minors", etc. (e.g. those who have not reached their 18th or 21st birthday according to the rules of the applicable jurisdictional domain).

[ISO/IEC 15944-5:2008 (3.113)]

3.122
publicly available personal information
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 Examples of 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 Examples of 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.

[ISO/IEC 15944-8 (3.118)]

3.123
recognized individual identity (rii) (in LET privacy protection)
identity of an **individual**, i.e., **individual identity**, established to the extent necessary for the specific purpose of a **learning transaction**

NOTE Adapted from ISO/IEC 15944-8.

3.124
recognized individual name (RIN)
persona of an **individual** having the properties of a **legally recognized name (LRN)**

NOTE 1 On the whole, a persona presented by an individual should have a basis in law (or recognized jurisdictional domain) in order to be considered as the basis for a recognized individual name (RIN).

NOTE 2 An individual may have more than one RIN and more than one RIN at the same time.

NOTE 3 The establishment of a RIN is usually accompanied by the assignment of a unique identifier, i.e. by the jurisdictional domain (or public administration) which recognizes the persona as a RIN.

[ISO/IEC 15944-5:2008 (3.114)]

3.125
recognized Person identity (rPi) (in LET privacy protection)
identity of a **Person**, i.e., **Person identity**, established to the extent necessary for a specific purpose in a **learning transaction**

NOTE Adapted from ISO/IEC 15944-1.

3.126
recorded information
any **information** that is recorded on or in a **medium** irrespective of form, recording **medium** or technology used, and in a manner allowing for storage and retrieval

NOTE 1 This is a generic definition and is independent of any ontology, (e.g., those of "facts" versus "data" versus "information" versus "intelligence" versus "knowledge", etc.).

NOTE 2 Through the use of the term "information," all attributes of this term are inherited in this definition.

NOTE 3 This definition covers:

(i) any form of recorded information, means of recording, and any medium on which information can be recorded; and,
(ii) all types of recorded information including all data types, instructions or software, databases, etc.

[ISO/IEC 15944-1:2011 (3.56)]

3.127
register
set of files containing **identifiers** assigned to items with descriptions of the associated items

[ISO 19135:2005 (4.1.9)]

3.128
registration
rule-based **process**, explicitly stated, involving the use of one or more **data elements**, whose value (or combination of values) are used to identify uniquely the results of assigning an OeRI

[ISO/IEC 15944-2:2006 (3.95)]

3.129
Registration Authority (RA)
Person responsible for the maintenance of one or more **Registration Schemas (RS)** including the assignment of a unique **identifier** for each recognized entity in a **Registration Schema (RS)**

[ISO/IEC 15944-1:2011 (3.57)]

3.130
Registration Authority Identifier (RAI)
identifier assigned to a **Registration Authority (RA)**

[ISO/IEC 11179-1:2004 (3.3.32)]

3.131
Registration Schema (RS)
formal **definition** of a set of **rules** governing the **data** fields for the description of an **entity** and the allowable contents of those fields, including the **rules** for the assignment of **identifiers**

[ISO/IEC 15944-1:2011 (3.58)]

3.132
Registration Schema (based) – recognized individual identity (RS-rii) (in LET privacy protection)
recognized individual identity (rii) for use in a **learning transaction**, by the buyer as an **individual**, which is one based on the use by an **individual** as a member of a specified **Registration Schema (RS)** of a particular **Registration Authority (RA)**

NOTE Adapted from ISO/IEC 15944-8.

3.133
registry
information system on which a **register** is maintained

[ISO/IEC 15944-2:2006 (3.99)]

3.134
regulator
Person who has authority to prescribe **external constraints** which serve as **principles**, policies or **rules** governing or prescribing the behaviour of **Persons** involved in a **learning transaction** as well as the provisioning of goods, services, and/or rights interchanged

NOTE Adapted from ISO/IEC 15944-1.

3.135
regulatory learning transaction (RLT)
class of **learning transactions** for which the explicitly shared goal has been established and specified by a **jurisdictional domain**, as a **Person** in the role of a **regulator**

NOTE 1 A regulatory learning transaction (RLT) can itself be modelled as a stand-alone learning transaction and associated scenario(s). For example, the filing of a tax return, the making of a customs declaration, the request for and issuance of a license, the provision of a specified service of a public administration, a mandatory filing of any kind with a regulator, etc.

NOTE 2 A regulatory learning transaction (modelled as a scenario) can form part of another learning transaction.

NOTE 3 A RLT may apply to a LET provider only, a learner only or both, as well as any combination of parties to a learning transaction.

NOTE 4 A RLT may require or prohibit the use of an agent or third party.

NOTE 5 A regulatory learning transaction (RLT) may be specific to the nature of the good, services and/or right forming part of a learning transaction.

NOTE 6 Adapted from ISO/IEC 15944-5.

3.136
retention period
length of time for which **data** on a **data medium** is to be preserved

[ISO/IEC 2382-12:1988 (12.04.01)]

3.137
role
specification which models an external intended behaviour (as allowed within a **scenario**) of an **Open-edi Party**

[ISO/IEC 14662: 2010 (3.25)]

3.138
rule
statement governing conduct, procedure, conditions and relations

NOTE 1 Rules specify conditions that must be complied with. These may include relations among objects and their attributes.

NOTE 2 Rules are of a mandatory or conditional nature.

NOTE 3 In Open-edi, rules formally specify the commitment(s) and role(s) of the parties involved, and the expected behaviour(s) of the parties involved as seen by other parties involved in (electronic) learning transactions. Such rules are applied to: (a) content of the information flows in the form of precise and computer-processable meaning, i.e. the semantics of data; and, (b) the order and behaviour of the information flows themselves.

NOTE 4 Rules must be clear and explicit enough to be understood by all parties to a learning transaction. Rules also must be capable of being able to be specified using a using a Formal Description Technique(s) (FDTs).

EXAMPLE A current and widely used FDT is "Unified Modelling Language (UML)".

NOTE 5 Specification of rules in an Open-edi transaction should be compliant with the requirements of ISO/IEC 15944-3 "Open-edi Description Techniques (OeDT)".

[ISO/IEC 15944-2:2006 (3.101)]

3.139
rulebase
pre-established set of **rules** which interwork and which together form an autonomous whole

NOTE One considers a rulebase to be to rules as database is to data.

[ISO/IEC 15944-2:2006 (3.102)]

3.140
scenario attribute
formal specification of information, relevant to an **Open-edi scenario** as a whole, which is neither specific to **roles** nor to **Information Bundles**

[ISO/IEC 14662:2010 (3.26)]

3.141
scenario component
one of the three fundamental elements of a scenario, namely **role**, **information bundle**, and **semantic component**

[ISO/IEC 15944-2:2006 (3.104)]

3.142
scenario content
set of recorded information containing **registry** entry **identifiers**, labels and their associated **definitions** and related **recorded information** posted (or reposted) in any **registry** for **business** objects

[ISO/IEC 15944-2:2006 (3.105)]

3.143
scenario specification attribute
any **attribute** of a scenario, role, **Information Bundle**, and/or **semantic component**

[ISO/IEC 15944-2:2006 (3.106)]

3.144
SC identifier
unique, linguistically neutral, **unambiguous**, referenceable **identifier** of a **Semantic Component**

[ISO/IEC 15944-2:2006 (3.107)]

3.145
seller
Person who aims to hand over voluntarily or in response to a demand, a Good, service and/or right to another **Person** and in return receives an acceptable equivalent value, usually in money, for the Good, service and/or right provided

[ISO/IEC 15944-1:2011 (3.62)]

3.146
Semantic Component (SC)
unit of **recorded information** unambiguously defined in the context of the learning goal of the **learning transaction**

NOTE 1 A SC may be atomic or composed of other SCs.

NOTE 2 Adapted from ISO/IEC 14662.

3.147
semantic identifier (SI)
IT-interface **identifier** for a **semantic component** or other semantic for which (1) the associated context, applicable **rules** and/or possible uses as a semantic are predefined and structured and the **Source Authority** for the applicable **rulebase** is identified (as per Part 5); and (2) for which more than one or more **Human Interface Equivalents (HIEs)** exist

NOTE The identifier for a Semantic Component (SC), an Information Bundle (IB) and/or an ID Code for which one or more Human Interface Equivalents (HIEs) exist are considered to have the properties or behaviours of semantic identifiers.

[ISO/IEC 15944-5:2008 (3.136)]

3.148
set of recorded information (SRI)
recorded information of an **organization** or **public administration**, which is under the control of the same and which is treated as a unit in its information life cycle

NOTE 1 A SRI can be a physical or digital document, a record, a file, etc., that can be read, perceived or heard by a person or computer system or similar device.

NOTE 2 A SRI is a unit of recorded information that is unambiguously defined in the context of the business goals of the organization, i.e., a semantic component.

NOTE 3 A SRI can be self-standing (atomic), or a SRI can consist of a bundling of two or more SRIs into another “new” SRI. Both types can exist simultaneously within the information management systems of an organization.

[ISO/IEC 15944-5:2008 (3.137)]

3.149
Source Authority (SA)
Person recognized by other **Persons** as the authoritative source for a set of **constraints**

NOTE 1 A Person as a Source Authority for internal constraints may be an individual, organization, or public administration.

NOTE 2 A Person as Source Authority for external constraints may be an organization or public administration.

EXAMPLE In the field of air travel and transportation, IATA as a Source Authority, is an "organization," while ICAO as a Source Authority, is a "public administration".

NOTE 3 A Person as an individual shall not be a Source Authority for external constraints.

NOTE 4 Source Authorities are often the issuing authority for identifiers (or composite identifiers) for use in learning transactions.

NOTE 5 A Source Authority can undertake the role of Registration Authority or have this role undertaken on its behalf by another Person.

NOTE 6 Where the sets of constraints of a Source Authority control a coded domain, the SA has the role of a coded domain Source Authority.

[ISO/IEC 15944-2:2006 (3.109)]

3.150
special language
language for special purposes (LSP), **language** used in a subject field and characterized by the use of specific linguistic means of expression

NOTE The specific linguistic means of expression always include subject-specific terminology and phraseology and also may cover stylistic or syntactic features.

[ISO 1087-1:2000 (3.1.3)]

3.151
standard
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

NOTE This is the generic definition of "standard" of the ISO and IEC (and found in the ISO/IEC JTC1 Directives, Part 1, Section 2.5:1998). {See also ISO/IEC Guide 2: 1996 (1.7)}

[ISO/IEC 15944-1:2002 (3.64)]

3.152
term
designation of a defined **concept** in a special **language** by a linguistic expression

NOTE A term may consist of one or more words i.e. simple term, or complex term or even contain symbols.

[ISO 1087:2000 (5.3.1.2)]

3.153
text
data in the form of **characters**, symbols, words, phrases, paragraphs, sentences, tables, or other **character** arrangements, intended to convey a meaning and whose interpretation is essentially based upon the reader's knowledge of some **natural language** or **artificial language**

EXAMPLE A business letter printed on paper or displayed on a screen.

[ISO/IEC 2382-23:1994 (23.01.01)]

3.154
third party (in LET privacy protection)
Person besides the two primarily concerned in a **learning transaction** who is **agent** of neither and who fulfils a specified **role** or function as mutually agreed to by the two primary **Persons** or as a result of **external constraints**

NOTE 1 It is understood that more than two Persons can at times be primary parties in a learning transaction.

NOTE 2 Adapted from ISO/IEC 15944-1.

3.155
treaty
international agreement concluded between **jurisdictional domains** in written form and governed by international law

NOTE 1 On the whole a treaty is concluded among UN member states.

NOTE 2 Treaties among UN member states when coming into force are required to be transmitted to the Secretariat of the United Nations for registration or filing or recording as the case may be and for publication. {See further Article 80 or the Charter of the UN}

NOTE 3 Treaties can also be entered into by jurisdictional domains other than UN member states, i.e., non-members such as international organizations and the rare sub-national units of federations which are constitutionally empowered to do so.

NOTE 4 A treaty can be embodied in a single instrument or in two or more related instruments and whatever it particular designations. However, each treaty is a single entity.

NOTE 5 Jurisdictional domains can make agreements which they do not mean to be legally binding for reasons of administrative convenience or expressions of political intent only, (e.g., as a Memorandum of Understanding (MOU)).

NOTE 6 Adapted from the Vienna Convention on the Law of Treaties, 1(a).

[ISO/IEC 15944-5:2008 (3.144)]

3.156
truncated name
short form of a **name** or **persona** of a **Person** resulting from the application of a **rule**-based **truncation process**

[ISO/IEC 15944-5:2008 (3.145)]

3.157
truncated recognized name (TRN)
truncated name, i.e., **persona**, of a **Person** which has the properties of a **legally recognized name (LRN)**

NOTE 1 Truncated recognized name(s) may be required for use in machine-readable travel documents, (e.g., passports or visas), identity tokens, drivers' licenses, medicare cards, etc.).

NOTE 2 The source of a truncated recognized name may be a legally recognized name.

[ISO/IEC 15944-5:2008 (3.146)]

3.158
truncation
rule-base **process**, explicitly stated, for shortening an existing **name** of an **entity** to fit within a predefined maximum length (of **characters**)

NOTE Truncation may be required for the use of names in IT systems, electronic data interchange (EDI), the use of labels in packaging, in the formation of a Person identity (Pi), etc.

[ISO/IEC 15944-5:2008 (3.147)]

3.159
unambiguous (in LET privacy protection)
level of certainty and explicitness required in the completeness of the semantics of the **recorded information** interchanged appropriate to the goal of a **learning transaction**

NOTE Adapted from ISO/IEC 15944-1.

3.160
vendor
seller on whom **consumer protection** requirements are applied as a set of **external constraints** on a **learning transaction**

NOTE 1 Consumer protection is a set of explicitly defined rights and obligations applicable as external constraints on a learning transaction.

NOTE 2 It is recognized that external constraints on a seller of the nature of consumer protection may be peculiar to a specified jurisdictional domain.

NOTE 3 Adapted from ISO/IEC 15944-1.

3.161
vocabulary
terminological **dictionary** which contains **designations** and **definitions** for one or more specific subject fields

NOTE The vocabulary may be monolingual, bilingual or multilingual.

[ISO 1087-1:2000 (13.7.2)]

4 Symbols and acronyms

For the purpose of this document, the following symbols and acronyms apply.

Acronym	Description
AHP	Ad-Hoc on Privacy (of SC36)
APEC	Asia-Pacific Economic Cooperation
API	Application Programming Interface
BOV	Business Operational View
BTI	Learning transaction Identifier
BTM	Learning transaction Model
cdRS	coded domain Registration Schema
cdSA	coded domain Source Authority
CV	controlled vocabulary
DMA	Decision Making Application
DMA Interface	Decision Making Application Interface
EC	European Community
EDI	Electronic Data Interchange
EU	European Union
FDT	Formal Description Technique
FSV	Functional Service View
HIE	Human Interface Equivalent
IAA	individual accessibility agent
IB	Information Bundle
ICT	Information communication and telecommunication
ID	identification
IEC	International Electrotechnical Commission
ii	individual identity
ILCM	information life cycle management
IPD	Information Processing Domain
ipRS	individual persona Registration Schema
IRBOI	International Registration Business Object Identifier
ISO	International Organization for Standardization
IT System	Information Technology System
ITLET	Information technology for Learning Education and Training
ITU	International Telecommunications Union
ITU-R	International Telecommunications Union – Radiocommunications Sector
ITU-T	International Telecommunications Union – Telecommunications Sector
JTC1	Joint Technical Committee 1 “Information Technology” (of the ISO and IEC)
LET	learning, education and training
LET- FSV	LET – Functional Services View
LET-OV	LET operational view
LipRS	legally (recognized) individual persona Registration Schema
LRII	legally recognized individual identity
LRL	Legally Recognized Language
LRN	Legally Recognized Name
LTI	Learning Transaction Identifier

Acronym	Description
LTM	Learner Transaction Model
md-rii	mutually defined – recognized individual identity
NAFTA	North American Free Trade Agreement
NWIP	New Work Item Proposal
OeBTO	Open-edi Learning transaction Ontology
OECD	Organization for Economic Co-operation and Development
OeDT	Open-edi Descriptive Techniques
OeORI	Open-edi Registration Organization Identifier
OeP	Open-edi Party
OeR	Open-edi Registry
OeRA	Open-edi Registration Authority
OeRI	Open-edi Registry Item
OeRO	Open-edi Registration Organization
OeRR	Open-edi Records Retention
OeS	Open-edi scenario
OeSI	Open-edi Support Infrastructure
PCS	privacy collaboration space
Pi	Person identifier
PPO	Privacy Protection Office
pRS	persona Registration Schema
RA	Registration Authority
RAI	Registration Authority Identifier
RBT	Regulatory Learning transaction
rii	recognized individual identity
RIN	Recognized Individual Name
rPi	recognized Person identity
RA	Registration Authority
RLT	regulatory learning transaction
RS	Registration Schema
RS-rii	Registration Schema (based) – recognized individual identity
SA	Source Authority
SC	Semantic Component
SCS	semantic collaboration space
SI	Semantic Identifier
SRI	set of recorded information
TRN	truncated recognized name
UML	Unified Modelling Language
UN	United Nations
UN/ECE	UN Economic Commission for Europe
URI	Universal Resource Locator

5 Fundamental principles and assumptions governing privacy protection requirements in learning transactions involving individual learners (external constraints perspective)

5.1 Introduction and sources of requirements

Whilst there is acknowledgement that information must, of necessity, be exchanged in the furtherance of the goals and actualization of a learning transaction, many jurisdictional domains require that where personal information is concerned particular external constraints apply, i.e., those which involve an individual learner as a party to a learning transaction.

Although legislation and regulations of a privacy/data protection nature differ among the many jurisdictional domains where they exist, on the whole, there are many "generic" elements. A high level review and analysis of privacy/data protection legislation in Australia, Canada, Japan, USA, (and APEC member states), the EU, and Norway as well as Europe (both at the EU level, and that of component countries (and within country such as those of länder within Germany, provinces/territories in Canada, etc.), indicates that all these laws and regulations have common primitive requirements. These are captured and integrated below into a single set of common privacy protection principles.

The essential aspects of each of these eleven (11) common privacy protection principles and their requirements are captured below along with associates of rules[18)] It is noted that for LET providers and public administrations to be able to comply with these rules as external constraints, which apply to them, they have to ensure that their surrounding and overarching learning processes and IT systems may be required to be changed to be able to support external constraints of this nature.

The three most common and international recognized and accepted sources for privacy protection requirements are:

1) the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data / Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel[19)]

2) the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data / Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[20)]

3) the 2005 APEC Privacy Framework[21)]

---

18) The development of the Part 1 of the multipart ISO/IEC 29187 set of privacy protection and LET standard standards focuses on common primitives which are captured in the form of principles and their rules along with clearly defined concepts, i.e., as a rule-based approach in support of the Learning Operational View.

19) http://www.oecd.org/document/53/0,3343,fr_2649_34255_15591797_1_1_1_1,00.html.

20) this 1995 directive is supplemented by the directive 2002/58/ec of the european parliament and of the council of 12 july 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications) / directive 2002/58/ce du parlement européen et du conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques directive vie privée et communications électroniques) http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

21) http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

These three normative references, i.e., as referenced specifications are indispensible to the understanding and use of this document. In addition, the following three normative references are also essential to the understanding and use of this Part of ISO/IEC 29187 and shall be used; namely:

a) the Charter of the United Nations;

b) the UN Convention on the Rights of Persons with Disabilities; and,

c) the Vienna Convention on the Law of Treaties.

The approach to the development of the 11 principles governing privacy protection requirements is illustrated in the following Figure 2.

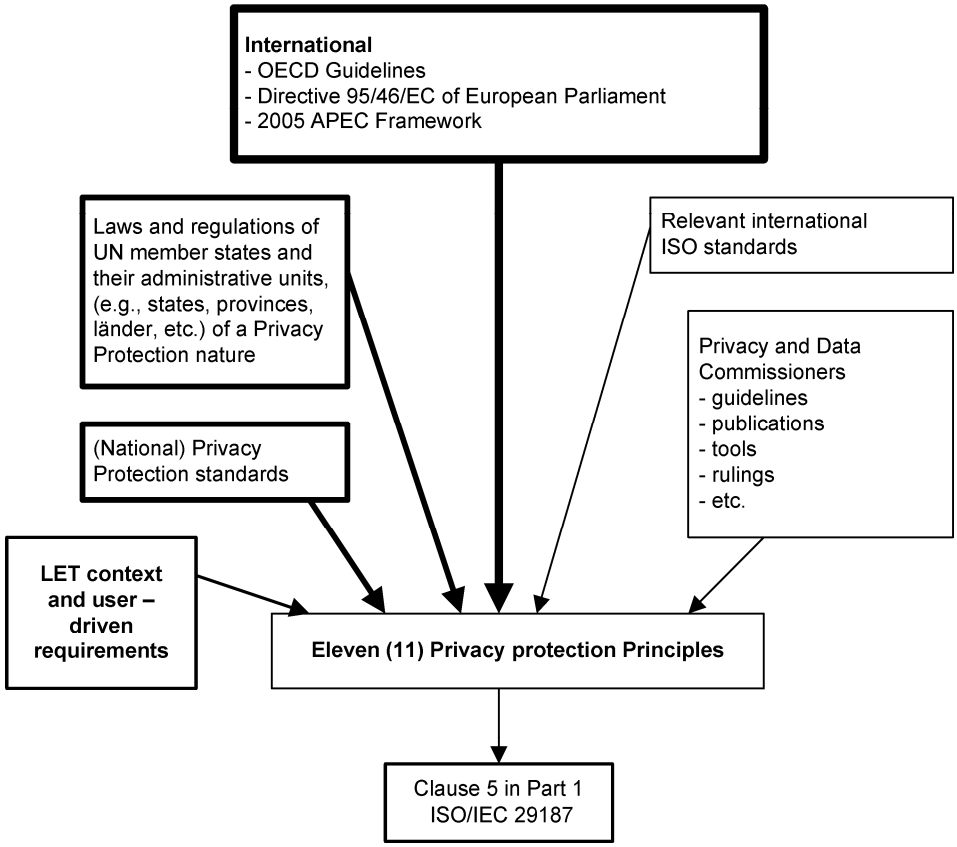

Figure 2 — Primary Sources for Privacy Protection Principles

In the text which follows, these eleven (11) Privacy Protection principles are placed in a LET and learning transaction context, i.e. that of the parties making a commitment on a commonly agreed upon goal for a learning transaction.

From a LET-FSV perspective, this includes ensuring that the IT systems of an LET provider provide the technical implementation measures which must be capable of exchanging the necessary information among the parties to a learning transaction. This is necessary to be able to determine when personal information is to be processed as against all other recorded information forming part of the learning transaction. This includes ensuring that applicable controls are in place in the Decision Making Applications (DMAs) of the IT systems of LET providers (and public administration) where personal information is processed and interchanged among all parties to a learning transaction[22)].

Finally, the privacy protection principles enumerated below represent an integrated whole therefore they should be interpreted and implemented as a whole and not piecemeal. Here one should note that in subsequent clauses of this standard, two or more of the privacy protection principles referenced often apply at the same time.

5.2 Exceptions to the application of the privacy protection principles

Privacy protection requirements of jurisdictional domains may contain exceptions (derogations) to the application of external constraints of this nature. The most common exceptions are those relating to national sovereignty and security, law enforcement, public safety and health. Exceptions of this nature often requires access to personal information about a particular individual learner and the tracing of any other personal information pertaining to that individual learner[23)] (e.g., access to personal information by particular Persons other than those who are parties to the learning transaction, i.e., qualified and specified public administrations based on predefined criteria).

Rule 001:
Where exceptions to the application of privacy protection principles exist, they shall be:

1) **limited and proportional [24)] to meeting the objectives to which these exceptions relate; and,**
   a) **made known to the public; or,**
   b) **in accordance with law.**

---

22) On Decision Making Applications (DMAs), Information Processing Domain (IPD) and Open-edi Support Infrastructure (OeSI) in IT systems, see further Clause 5.2 *Functional Service View* in ISO/IEC 14662:2010 (3rd edition) and its Figure 3 *Open-edi system relationships*.

23) Traceability issues including those pertaining to individuals are being addressed in the ISO/IEC 15944-9 "Traceability Framework" standard which is under development.

24) In relation to "limited and proportional", the *APEC Privacy Framework*, Clause 13 states that "The Principles contained in Part III of the APEC Privacy Framework should be interpreted as a whole rather than individually, as there is a close relationship among them". It goes on to state that countries implementing the Framework "may adopt suitable exceptions that suit their particular circumstances". Further, "one should take into consideration the impact of these activities", i.e. invocation of an exception, "upon the rights, responsibilities and legitimate interests of individuals".

5.3 Fundamental Privacy Protection Principles[25)]

5.3.1 Privacy Protection Principle 1: Preventing Harm

Rule 002:
The protection of personal information shall be designed to prevent the misuse of such personal information (acknowledging the risk that harm may result from such misuse of personal information

A primary objective of the preventing harm principle is to prevent misuse of personal information, and consequently harm to individual learners[26)] Therefore, the implementation of privacy protection, including self-regulatory efforts, education, and awareness campaigns, as well as enforcement mechanisms, etc., should be a priority governance principle of any LET provider. This applies to both its learning operational view (LOV) and functional services view (FSV) of the LET provider, and especially to the interchange of personal information among parties to a learning transaction.

Guideline 002G1:
Acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk and remedial measures should be proportionate to the likelihood and severing of the harm threatened by the collection of personal information.

5.3.2 Privacy Protection Principle 2: Accountability

Rule 003:
An LET provider subject to privacy protection requirements in the jurisdictional domain (at whatever level[27)] in which it provides a LET good, service and/or rights, shall have in place implemented, enforceable policies and procedures with proper accountability controls required to ensure its compliance with applicable privacy protection requirements.

This means that the ability to comply to applicable privacy protection requirements is a precondition for an LET provider to be able to offer goods, services and/or rights to individual learners in that jurisdictional domain.

[25)] The purpose here is simply to present, in summary form and in a non-technical LOV manner, key common privacy/data protection requirements as promulgated. Other groupings of Privacy/Data Protection Principles have been published elsewhere; and some may have more or fewer than these ten “principles”. The same set of requirements can also be grouped differently or have different titles.

[26)] This privacy protection principle is introduced in the *APEC Privacy Framework*. It can be considered an application of the generic aspect of the human right of “do no harm”, already a well and long established principle in the field of medicine.

[27)] In some jurisdictional domains, privacy protection requirements are found at the UN member state level, an administrative unit of the UN member state, and/or at the municipal level or any combination of the same.

Rule 004:
An LET provider[28] is responsible for all personal information under its control and shall designate an organization Person, i.e. a privacy protection officer (PPO), who is accountable for the LET provider'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(s) in which the LET provider operates.

> **privacy protection officer (PPO)**
>
> ***organization Person*** authorized by the ***organization*** to act on behalf of that ***organization*** and entrusted by the ***organization*** as the officer responsible for the overall governance and implementation of the privacy protection requirements for information life cycle management not only within that ***organization*** but also with respect to any ***electronic data interchange*** of ***personal information*** on the ***individual*** concerned with parties to the ***learning transaction***, including a ***regulator*** where required, as well as any ***agents, third parties*** involved in that ***learning transaction***
>
> *[adapted from ISO/IEC 15944-8, 3.109]*

In practice, this means that at any time, in the process of an individual learner establishing a learning transaction with an organization or public administration (or vice-versa), that the individual learner is informed of the privacy protection officer (PPO) within the organization who has been assigned this role[29] Most organizations already do so in the planning phase of the process for a learning transaction by making such information readily available in their catalogue, on their website, etc.

Rule 005:
Any organization to which privacy protection requirements apply shall have in place policies and practices which make clear as to who and where, and in an enforceable and auditable manner in their LET operations is responsible for compliance with these external constraints as applicable to the conduct of learning transactions where the individual learner is a party to a learning transaction.

Guideline 005G1
Organizations should ensure that their accountability policies, practices and controls are supported, if not imbedded, in the operations of their DMAs in their IT systems to ensure that personal information of individual learners is managed through it information life cycle in compliance with applicable privacy protection requirements.

---

[28] The use of the term "organization" in these Privacy Protection Principles includes "public administration".

[29] Within an organization it is a common and well accepted practice to label any organization Person who has a (legal) responsibility at the organization–wide level as an "officer", i.e., one who has an "official" responsibility on behalf of the organization as a whole. The concept/term "controller" within an organization is usually related to "financial controls".

It is recognized “best practice” that the design and operation of an organizations IT systems in support of its LET operations should implement not only the information management polices of the organization but also, and especially, any external constraints which may apply. In this context, privacy protection requirements represent a defined set of external constraints of jurisdictional domains which apply when and where an individual learner is involved.[30)] It is not uncommon that in the actualization of a learning transaction that the LET provider utilizes one or more “agents”, referred to at times as “outsourcing”. The role of such agent may range from a simple registration role to undertaking of many other LET operational functions. At the same time, it is also not uncommon that the actualization of the learning transaction involves the use of third parties. The use and role of third parties may be mutually consented to by the individual learner and LET provider, i.e. as part of modelling internal constraints, or be mandatory based on the requirements of an applicable regulator, i.e. as external constraints to a learning transaction.

Privacy protection requirements which apply to the organization when providing a LET good, service and/or right to an individual learner are mute on the aspect of delegation (e.g. via subcontractors) of role or functions in a learning transaction to an agent or third party. Commonly, the organization acting as the LET provider, i.e., as primary party to a learning transaction, remain responsible and accountable for ensuring that privacy protection requirements are complied with for that learning transaction by the involved agent(s) or third party(ies).

Rule 006:
Where an organization, as a LET provider, delegates any aspect of a learning transaction involving an individual learner , and interchanges of personal information pertaining to that individual learner, to an “agent” (and/or “third party”), the organization shall ensure,

1) **that in its arrangement with the designated agent (and/or third party), the agent (and/or third party) is fully aware of; and,**

2) **commits itself to support the privacy protection requirements pertaining to the learning transaction[31)]**

This rule is consistent with the overall approach that delegation of LOV or LET-FSV aspects (including scenario components) to an agent (and/or third party) of commitments made by a Person as a LET provider in a learning transaction apply to any combination of agents and/or third parties where the LET provider may delegate a LOV or FSV aspect to them. It is noted that should an LET provider make use of an agent in the instantiation of a learning transaction involving an individual learner, and thus personal information is involved, that the LET provider remains responsible for ensuring that privacy protection requirements are complied with.

Guideline 006G1
Prior to an LET provider delegating part of the instantiation of a learning transaction to an agent, the LET provider should obtain (written) assurance of the “agent’s compliance with privacy protection requirements and particularly in the DMAs in the IT systems of the agent.

With respect to the engagement of a third part in a learning transaction, it is noted that a third party is not an agent of either the individual learner or the LET provider whether a third party is one who fulfils a specific role or function in the execution of a learning transaction as mutually agreed to by the two primary Persons or as a result of applicable external constraints.

---

30) Privacy protection is but one set of external constraints of a public policy nature which apply in a learning transaction which involves an individual learner. Others include those of a consumer protection, individual accessibility, etc., nature. See further below Clause 7 *Public policy requirements of jurisdictional domains on a learning transaction*.

31) One should note that whether or not the LET provider in an learning transaction, decides to delegate one or more role or functions (if permitted in a scenario) to an agent and/or third party, that this is immaterial to the fact that the LET provider shall ensure that it maintains control of any and all of the personal information associated with a learning transaction involving an individual learner doing so in compliance with information life cycle management (ILCM) principles.

Guideline 006G2
Where a third party is involved in a learning transaction involving personal information , the LET provider and individual learner should be provided with the (written) assurance of the "third party's compliance with privacy protection requirements and particularly in the DMAs in the IT systems of the third party.

Guideline 006G3

Where :

1) **due to the nature of the LET good, service and/or right of the goal of the learning transaction, external constraints of a jurisdictional domain mandate the use of a third party; and,**

2) **for a learning transaction of this nature, involving an individual learner, the jurisdictional domain which is the source of such an external constraint should ensure that such a third party is able to comply with privacy protection requirements and particularly in the DMAs in the IT systems of the third party.**

Rule 007:
An agent (and/or third party) which commits itself to act on behalf of a Person acting as a LET provider in a learning transaction involving an individual learner, in a jurisdictional domain where privacy protection requirements apply, shall ensure that in its DMA()s in its IT system(s) is capable of supporting applicable external constraints requirements.

The purpose of this rule is to ensure that any agent (and/or third party) recognizes the fact that it as a Person in a jurisdictional domain is also bound by external constraints of a privacy protection nature which apply to that jurisdictional domain. This applies to any learning transaction where the involving an individual learner and thus privacy protection requirements apply. This also applies to applicable data synchronizations requirements between the LET providers and its agent(s) and/or third-party (ies).

Rule 008:
A LET provider shall ensure that in the execution of an (instantiated) learning transaction, i.e., as identified by its learning transaction identifier (LTI), that where these involve parties, other than the individual learner, that such parties, are capable of and have implemented the requirements of the privacy protection principles[32)]

It is recognized that the development of efficient and cost-effective Open-edi scenarios often require EDI among parties with varying LET relationships. It is therefore not uncommon that the Person acting as a Person, in a learning transaction, involves other Persons in the instantiation of the learning transaction. It is important for a LET provider acting as a LET provider in a learning transaction to ensure that these other parties to a learning transaction are committed to and do have in place (and have implemented) applicable privacy protection requirements, i.e. for any learning transaction involving an individual learner.

Finally, one should note that there is a direct relation here between accountability requirements and requirements here of synchronization of master data among all the parties to a learning transaction. {Some of these are identified below in Annex C below as part of ILCM requirements}

The internal constraint of the general requirement of data synchronization with master data among parties to a learning transaction becomes an external constraint based on privacy protection principles where this involves an individual learner and thus requiring data synchronization.

---

32) A key requirement is the ability for the LET provider to be able to support data synchronization among the IT systems of all parties participating in a learning transaction. This is particularly important where this data is of the nature of personal information.

5.3.3 Privacy Protection Principle 3: Identifying Purposes

Rule 009:
The specified purpose(s) for which personal information is collected with respect to the (the (potential) goal of the learning transaction shall be identified by the LET provider at or before the personal information is collected.

Here the specified purpose is deemed to be the goal of the learning transaction, i.e., that which is mutually agreed to by the individual learner at the end of the negotiation phase (and prior to the actualization) phase.

In an Open-edi context, the purpose for which the personal information is being collected is specified as (part of) the purpose of an Open-edi scenario, i.e., as the OeS purpose. The Clause 7.2 Rules for scoping Open-edi scenarios in ISO/IEC 15944-1 already make provision for supporting this rule from a privacy protection requirements perspective.[33)]

5.3.4 Privacy Protection Principle 4: Informed Consent

The principle of "informed consent" requires that the individual, as prospective individual learner, be fully and explicitly informed by the LET provider as to why and for what purpose, the individual is requested (or required) to provide (additional) personal information (of various kinds), i.e., in addition to that which may be required with respect to payment aspects where applicable.

This principle is clearly a requirement to flag personal information supplied as being for limited use only. It is for the surrounding LOV and LET-FSV processes to identify what the use implications are, and how the 'informed consent' status for the learning transaction has been achieved. However, it is clearly necessary for scenarios to develop the granularity of what the informed consent being given actually is for. It is possible that different data in a single transaction could be of different "informed consent" use; however, this standard addresses the simplest case of all of the data to the transaction being subject to the single 'informed consent' agreement.

It is noted that in a substantial number of learning transaction, the individual learner remains for all practical purposes "anonymous". A good is purchased in a store, payment is made in cash or by credit/debit card (as authorized by the relevant financial institution, etc. and the LET provided by the LET provider of a sales receipt which contains the associated learning transaction identifier (LTI). As such the only binding between the individual as individual learner and the LET provider might be the LTI[34)] Thus the use of a LTI is mandatory.[35)]

Rule 010:
Where in a learning transaction, the LET provider requires the individual learner to provide personal information, the LET provider shall ensure that the collection and use of such personal information shall have the informed and explicit consent of the individual learner and that the same be directly linked to the specified goal of the learning transaction (to be) entered into.

---

33) See further below Clause 12.3 "*Template for specifying an Open-edi scenario"* of privacy protection requirements" in ISO/IEC 15944-8:2011

34) In the development of this standard, one has taken into account that many LET providers, especially small and medium sized LET providers do not collect or maintain personal information pertaining to an individual learner apart from basic personal information including that required to be collected and maintained by a regulator. It is also a common learning practices that with respect to any complaint, return of (mandatory merchandise purchased, (e.g. laptops, books, learning packages, etc.), invocation of a warranty, that the individual learner (or now owner) must have the sales receipt (in hand) and/or be able to provide the LTI pertaining to the learning transaction.

35) On the role and importance of learning transaction identifier (LTI) and associated rules, see below Clause 11.2 *Learning Transaction Identifier*.

The application of this rule also covers to possible use of "automatic opt-in"[36] by the LET provider, i.e., they are not allowed unless expressly consented to be the individual learner , although that may not be part of the "informed consent" and may violate the principle of "limiting collection" and of "limiting use".This includes the need for a LET provider to ask for explicit consent from the individual learner, for the use of any of his/her personal information for any purpose which is different from that originally agreed to, i.e., as the agreed upon goal of the learning transaction. As such, privacy protection requirements preclude the use by the LET provider of an "automatic opt-ins" and in links (including posting any and use of Internet-based functional services which may be used to identify an individual learner). The following Guideline supports this privacy requirement.

Guideline 010G1:
In support of privacy protection requirements, the LET provider shall ensure that there are no "automatic opt-ins" by the LET provider with respect to aspects of the commitment exchange forming the basis of the learning transaction or any secondary use of the personal information of the individual who is the learner who is a party to a learning transaction.

Rule 011:
Any secondary use of personal information of the individual learner in a learning transaction requires the explicit and informed consent of the individual learner.

Here it is assumed that the LET provider in the role of LET provider will maintain a record (as a SRI) on the individual learner providing such explicit informed consent, i.e., in compliance with documentary evidence rules of the applicable jurisdictional domain.

The following Guideline represents a "best practice" approach[37]

Guideline 011G1:
Any use of "automatic opt-ins" shall be explicitly agreed to by the individual learner, i.e., as informed consent, and be recorded as such by the LET provider, i.e., in compliance with documentary evidentiary rules of the applicable jurisdictional domain.

This Guideline supports the fact that the use of "an automatic op-in" by a LET provider necessitates use of personal information of the individual learner and therefore requires documentary evidence of his/her informed consent.

Rule 012:
Except with the explicit informed consent of the individual learner or as required by law, personal information shall not be used or disclosed for purposes other than those for which it was collected, i.e., in the context of the specified goal of the learning transaction to which it pertains.

This means that:

- the personal information of the individual learner collected by the LET provider for that particular learning transaction shall not be disclosed, i.e., communicated to any other party(ies) unless so required for the actualization of that specific learning transaction (with the individual learner being fully informed of the same by the LET provider and having consented to the same);

- unless the individual learner provides explicitly stated and documented informed consent, none of the personal information created or obtained for one learning transaction shall be used for any other learning transaction or purpose (such as aggregation);

---

[36] With respect to rules governing the use of "automatic opt-in" by LET providers, there is a link here to external constraints of a privacy protection nature.

[37] Rules pertaining to compliance with documentary evidence rules of jurisdictional domains are outside the scope of this standard.

- once the learning transaction has been actualized all personal information shall be deleted unless required for post-actualization purposes and/or other specified external constraints of an information law nature require specific personal information to be retained; and,

- personal information concerning the transaction shall not be retained for longer that is necessary in the relevant jurisdiction for the purpose of satisfying national regulation for record keeping.

5.3.5 Privacy Protection Principle 5: Limiting Collection

Rule 013:
The collection of personal information shall be limited to only that which is necessary and relevant for the identified and specified purpose, i.e., the goal, of the specified learning transaction.

Only personal information on the individual learner that is essential, i.e., can be proved to be relevant, for the completion of the learning transaction "in hand" shall be collected. This also means that any information that is not essential to the learning transaction shall be clearly identified, and the learning transaction shall not fail if information that is not fundamental to the transaction is missing.

The implementation of this privacy protection principle requires that at the planning phase, or no later than before completion of the negotiation phase, in a learning transaction, that the individual learner is fully informed not only of the purpose of the learning transaction but also why specific sub-sets or components of personal information are required or optional, and that they are clearly and unambiguously identified.

Rule 014:
Any collection of personal information by the LET provider, or other parties to a learning transaction, which pertains to an individual learner in that learning transaction, shall be lawful and fair.

This rule recognizes the fact that:

1) laws (and regulations) of jurisdictional domains, i.e., external constraints, may require data to be collected depending on the nature of the LET good, service and/or right as the goal of the learning transaction; and,

2) where the (prospective) individual learner is a party to a learning transaction,

then that individual learner is required to provide specified personal information either as part of the actualization of a learning transaction or even during the planning, identification and/or negotiation phase, or at any time prior to the actualization of a learning transaction. For example, an external constraint may be of the nature that:

1) only an individual learner (and not a LET provider) may purchase a specified LET good, service and/or right; and,

2) where this is the case the individual learner may be required to provide additional personal information before making a purchase .This can include, the individual learner being required to provide proof of age, status (e.g. citizenship, landed immigrant, etc.), credentials (e.g. as a licensed medical doctor, an engineer, qualified technician, etc.).[38] This principle also provides that collection methods shall be lawful and fair. For example, fraudulent misrepresentation in order to obtain personal information on an individual learner is considered unlawful in most jurisdictional domains. This includes misrepresentation, via EDI, to deceive individual learners, as (potential) consumers to induce them to provide sensitive personal information such as credit/debit card numbers, bank account information, etc.[39]

Rule 015:
An LET provider collecting personal information shall inform the individual learner concerned whether or not the personal information collected is:

1) **essential to the intention of the learning transaction;**

2) **required to provided by the individual learner due to identified and specified constraints of jurisdictional domains applicable to the nature and goal of the learning transaction; and/or,**

3) **is "optional", i.e., desired to have by the LET provider acting as the LET provider but not required.**

5.3.6 Privacy Protection Principle 6: Limiting Use, Disclosure and Retention

This 6th Privacy Protection Principle consolidates and integrates what are considered "generic, primitive" Information Life Cycle Management (ILCM) principles which apply to any and all types of sets of recorded information (SRIs) within an LET provider (including public administrations) and among LET providers. This addresses the "collaboration space" among all parties, i.e., types of Person, to a learning transaction; As such, Annex D below titled "Integrated set of information life cycle management principles in support of information law compliance" applies to these privacy protection principles.[40] The integrated set of information life cycle management (ILCM) principles in support of information law compliance, which apply to data management and interchange generally also apply to Open-edi[41] within and among Persons (and their IT systems). In addition, Annex E below titled "Coded domains for the management and control of state changes, retention and destruction of personal information in commitment exchange, including learning transactions" supports both the implementation of the ILCM principles as well as privacy protection requirements.

---

[38] On this matter and for other examples see further, Clause 6.1.6 "*Learning model: Classes of External constraints",* Clause 6.3.3 *"Identification"* and Annex F, Clause F.2.3 "*Identification Phase*" in ISO/IEC 15944-1:2010.

[39] The use "unfair" includes of fraudulent means. The use of fraudulent means to obtain personal information on or about an individual (irrespective of how it may be used) is likely subject to sanctions under the Criminal Code (or laws of an equivalent nature) in most jurisdictional domains.

[40] The focus and scope of ISO/IEC JTC1/SC32 standards development work is *"Data Management and Interchange*" was at first only within and among the IT system(s) of a Person of primarily organizations (including public administrations) but now also includes individuals (and their IT systems). As such, Open-edi standards development, which focuses on the collaboration space among Persons and their IT systems, has from it inception, supported information life cycle management (ILCM) requirements in its standards development work. The need to reflect and support ILCM requirements is of particular importance where external constraints apply to the modelling of a learning transaction. This was reflected and explicitly supported in the development of the existing principles, rules and definitions in all the existing Parts of ISO/IEC 15944, i.e., its definitions of relevant concept, and rules and include those found in the "Characteristics of Open-edi", those pertaining to state changes, record retention, the specification of the collaboration space, etc., as well as being found in the templates for scoping Open-edi transactions and modelling Open-edi scenarios and their components.

As such Annex C below brings forward and states explicitly the ILCM principles in support of information law compliance, i.e. external constraints, applicable to the modelling of common learning transactions via Open-edi scenarios. Those ILCM principles also reflect good governance and best practices in information management and EDI.

[41] While the focus here is on "Electronic data interchange (EDI)", these ILCM principles apply to any internal or external constraints applicable to any. set of recorded information (SRI)of any Person

Rule 016:
The integrated set of ILCM principles applies to and supports the external constraints of a privacy protection nature for any learning transaction involving an individual learner and its personal information.

Parties to a learning transaction are required to be able to support these six Open-edi characteristics as requirements governing the DMAs of the LET provider in their IT systems[42)] The ILCM principles reflect and support the six key characteristics of Open-edi.

Note that this rule may require that some personal data must be retained specifically for this purpose and that this purpose is implicitly necessary to a transaction involving personal data.

Rule 017:
Personal information shall not be used or disclosed by the LET provider (or regulator) for purposes other than for those it was collected as part of the learning transaction, except with the informed consent of the individual learner, or as required by law. Secondary or derivative uses of personal information are not permitted.

This means that the purpose for which personal information was collected or requested from an individual learner shall be directly related to, if not explicitly stated, in the mutually agreed upon and explicitly stated goal of the learning transaction being instantiated.

In scenario definitions, this shall require that the scenario definition identify explicitly all data that are subject to this rule Other LOV processes will be required to enact this rule, so the scenario definition is required in order to identify to the party(ies) subject to this rule that they are liable for non-compliance if they fail to instantiate annual or other separate procedures in compliance with this rule.

Rule 019:
Where the LET provider, having collected personal information for a specific purpose and goal of the execution of the learning transaction, desires to use the relevant personal information for another purpose, it is necessary to obtain revised/new "informed consent" directly from the individual learner concerned.

This rule requires not only that:

1) the individual learner may refuse consent for a secondary, derivative or new use of its personal information; but also,

2) where an LET provider is not able to contact the individual learner concerned to make request for another use of that individual learner's personal information, then such a proposed "new" use is not permitted.

[42)] The six key characteristics by which Open-edi is recognized and defined are:

- actions based upon following rules;
- commitment of the parties involved;
- communications among parties automated;
- parties control and maintain their states;
- parties act autonomously; and,
- multiple simultaneous transactions can be supported.

See further Clause 5 "*Characteristics of Open-edi*" in ISO/IEC 15944-1.

Rule 020:
Personal information shall be retained by the LET provider only for as long as is necessary for the fulfillment of those purposes as specified as part of the learning transaction.

Personal information must be identified as having a specific 'life' of time of existence if this is to be other than that demanded for the purposes of national record keeping. This retention time period shall form part of the scenario definition and the time period will be explicit.

This also means that LET providers shall have in place auditable rules and procedures as are necessary to ensure that personal information no longer required for the post-actualization phase of a learning transaction shall be destroyed (expunged) by the LET provider, or its agents where applicable, and in a manner which can be verified via audit procedures.

For most, if not all, instantiated learning transactions, external constraints of the applicable jurisdictional domain(s) require that specific sets of recorded information(SRIs) pertaining to any learning transaction be retained by the LET provider for a specified period of time.

It is recognized that, depending on the nature of the LET good, service and/or right, which is the goal of the learning transaction, specified additional records retentions requirements of applicable jurisdictional domains may apply to all or specified subsets of all the recorded information pertaining to a learning transaction.

It is also recognized that where the purchase of a LET good, service and/or right involves "post-actualization" aspects of a temporal nature that these will also impact record retention requirements and obligations resulting from an actualized learning transaction. A primary example here of an internal constraint nature is that of a "warranty" for "n" number of years[43)] This includes the possibility that the individual learner who made the purchase may not be the "warranty holder"[44)]

In a LET context, LET providers are often required or have the long standing practice of retaining (summary) "student records" permanently, i.e., to be able to provide proof of completion of a certain level of primary, secondary schooling, obtaining a degree, a certificate, etc.

The following rules summarize these requirements from a LOV perspective:

Rule 021:
The LET provider shall identify to the individual learner any and all record retention requirements pertaining the resulting sets of recorded information which form part of the specified goal of a learning transaction as a result of applicable external constraints of jurisdictional domain(s) as a result of the actualization of the learning transaction.

Rule 022:
Where the LET provider offers a warranty (e.g. in relation to mandatory equipment purchase, software packages, etc.), or extended warranty, as part of the learning transaction, the LET provider shall inform the individual learner, of the associated added records retention requirements for the personal information associated with the warranty (including the purchase by the individual learner of an extended warranty).

The sale of many types of goods or services, require the LET provider to inform the individual learner of possible safety and health considerations with respect to whatever was purchased. These include product recalls, repairs, verifications checks or testing of specific function or components, etc.

---

43) Here it is noted that in order to be able to support a "warranty" of whatever nature, the LET provider will need to maintain personal information for a time period other, i.e. longer, than that required by law, i.e. as part of the applicable external constraints of the relevant jurisdictional domain(s). This is especially so where consumers purchase an "extended warranty".

44) For example, where the good or service purchased as a gift. Here the recipient of the gift, as an individual, would become the owner and also would complete the warranty information including personal information required for the warranty to be invoked.

Rule 023:
Where the individual learner in a learning transaction, the LET provider shall inform the individual learner of any and all records retention requirements of personal information which is recorded as the result of the actualization of the learning transaction, including:

1) **personal information which is required to actualize the learning transaction and the time period(s) for which such sets of personal information are to be retained;**

2) **additional personal information, i.e., in addition to (1), which is required to be collected and retained as a result of applicable external constraints, of whatever nature, of relevant jurisdictional domain(s); and/or,**

3) **additional personal information, i.e. in addition to (1) or (2), which is required to be collected and retained as a results of the invocation of an associated warranty, purchase of an extended warranty, or any other personal information which is required to be collected or retained as part of the post-actualization phase of an instantiated learning transaction.**

From a customer service, many LET providers, i.e. LET providers (including public administrations), wish to stay in contact with their customers for a variety of reasons. These include providing catalogues of their offerings, possible associated goods or services, etc., as well as obtaining client feedback, surveys, new product announcements, etc.

Rule 024:
Where the individual learner in learning transaction, the LET provider shall inform that individual learner of the applicable record retention conditions and especially where these pertain to personal information.

It is important that when the individual learner is a party to a learning transaction, prior to and at the actualization phase in a learning transaction,, that the individual learner is fully informed of the records retention requirements and practices of the LET provider particularly as these pertain to the personal information forming part of the set(s) of recorded information. Here it may well occur, depending on the nature of the learning transaction, that certain types of personal information may be subject to differing records retention periods.

It is noted that where the learning transaction is one of the nature of the provision of a service or a right, (e.g., a license of some kind) that the LET provider needs to retains a specified set(s) of personal information for as long as a learning transaction of this nature remains active.

Rule 025:
Where a learning transaction did not reach the actualization phase, any personal information collected by the LET provider in support of that transaction shall be deleted by the LET provider (unless the individual learner concerned explicitly consents to the prospective LET provider to the retention of such personal information for a defined period of time).

An individual learner may have provided personal information to a LET provider as part of the identification or negotiation phase. However, in this case the individual learner decided not to commit to the actualization of the learning transaction. As such the personal information provided by the individual learner to the LET provider is no longer relevant and therefore the LET provider concerned shall delete the personal information pertaining to that individual learner.

It is noted that this rule makes provision for the possibility that the individual, as a prospective individual learner, may consent to be kept informed by the LET provider about product information (e.g. via a catalogue), special sales, new offerings, etc. Such a decision by the individual learner is of the nature of obtaining “informed consent”.

Particular care must be taken to avoid collecting or providing data that are not actually necessary for the purpose(s) of the transaction itself. By way of example, in the transaction given in section 6 of a purchase and payment it may not be necessary for the LET provider to know the actual personal identity of the individual learner, but to have an identifier by which that individual learner may be uniquely identified to the LET provider. It may be sufficient that the LET provider is certain of payment because the LET provider has an authority from a third party such as a bank that the transaction will be paid. Thus the bank may need to know the identity of the individual learner and LET provider in order to fulfill its requirements in the transaction, whilst the LET provider does not need to know the identity of the individual learner[45)] The same is true when agents are used, or when a public administration is a supervisor to a transaction, where the other parties need to know and perhaps be able to prove that the public administration was involved, but not be able to identify the individual within the public administration actually involved (although the internal functions of the public administration may need that information for their own supervisory purposes).

5.3.7 Privacy Principle 7: Accuracy

It is to the mutual benefit of all parties to a learning transaction, and also a good learning practices, to ensure that any and all recorded information pertaining to a learning transaction be as timely, accurate, complete, up-to-date, etc., as possible. Accuracy of recorded information is an essential component of "integrity[46)] which is a major asset of any LET provider. No LET provider should keep recorded information on its learning transaction or its clients which is not accurate or out-of-date, especially in the DMAs of its IT systems. As such for this generally accepted set of internal constraint on recorded information applicable to all parties to a learning transaction, LET providers concluding learning transactions with individual learners, should have no difficulties in support the external constraint of "accuracy" of a privacy protection nature (including in the DMAs of their IT systems).

Rule 026:
Personal information shall be as accurate, complete and up-to-date as is necessary for the specified purposes for which it was collected in support of the learning transaction.

Here, the scenario definition shall make it clear that the data identified shall subsequently be capable of amendment (including deletion). It may be that there are other data for which alteration may be forbidden, either by automatic or manually inspired processes.
One should consider the implementation of this principle to be of the nature of good corporate governance and best practices. For a variety of reasons, LET provider should not retain personal information, or retain the same in its IT systems, if such personal information is not accurate, complete and up-to-date.

Guideline 026G1:

In order to support the privacy principle of accuracy, LET providers should consider informing their clients, who are individual learners, of the personal information retained on that individual learner, and do so on a cyclical basis in order to ascertain whether such personal information, collected earlier and still maintained by the LET provider, is still accurate.

---

45) An example here is the purchase by an individual of a LET software package, self-learn course material, etc., (especially where these do not involve the LET provider offering a degree, diploma, certificate, etc.).

46) It is noted that an organization which does not have policies and auditable procedures in place , as part of its overall governance, to ensure that the recorded information on which its decisions and commitments are made does not have the required level of "integrity" (e.g. timeliness, accuracy, being-up-to data, etc. and ensuring that all its recorded information which does not meet these criteria is expunged (unless required to be retained due to applicable external constraints), may find itself (and particular its officers) being subject to legal action for not exercising stewardship, due diligence, damages, etc., for not implementing these requirements (which in turn form part of the implementation of ILCM principles).

5.3.8 Privacy Protection Principle 8: Safeguards

This 8th privacy protection principle pertains to ensuring that the LET provider has in place policies operational controls and practices to ensure its policies pertaining to the retention, storage, preservation or destruction, confidentiality, integrity, continuity and availability of the processing, reproduction, distribution, sharing or other handling of its recorded information is "safeguarded" in compliance with applicable "information law" requirements.[47)]

This principle can be considered to be of the nature of an external constraint which makes such existing internal best practices from a learning operational view perspective mandatory from an external constraints privacy protection requirements perspective.

Recognized international standards for "safeguards" exist not only with respect to those pertaining to Open-edi but also in the fields of:

- records/information management (including records retention and archiving as well as supporting IT systems and their DMAs));
- audit controls;
- security services;
- "quality" of communication services;
- evidentiary aspects of paper, microform and/or electronic based document;
- database management;
- etc.

These international standards support and provide guidance to LET providers for addressing address and implementing most of the accountability, information managements, and "safeguard" requirements of a privacy protection nature. Many LET providers already have in place officers, mechanisms, procedures, etc., required to provide safeguard measures in support of the implementation of this principle either directly or as an integrated aspect of its overall approach to information management.

Rule 027:
Personal information shall be protected by operational procedures and safeguards and safeguards appropriate to the level of sensitivity of such recorded information and shall have in place (and tested) measures in support of compliance with privacy protection requirements of applicable jurisdictional domains, as well as any other external constraints which may apply such measures as are appropriate to ensure that all applicable legal requirements are supported.

Guideline 027G1:
Where an LET provider does not have a single designated focal point and "officer, i.e., a "privacy protection officer (PPO)" responsible for ensuring the identification and implementation of safeguard requirements applicable to all of its recorded information, it should ensure that all of its personal information meets privacy protection requirements.

This principle also introduces the concept of protection. Protection involves one or more constraints that are to be applied to specific data that are expected to provide the safeguard that is appropriate. It should be noted that the actual sensitivity of the data to be protected may be of national or cultural expectation, and need not be consistent. It should also be noted that in modelling, specific data fields are labelled with the protection that is to be provided, but that it is for the FSV implementation to determine how such protection requirements are given technical effect. In this standard only the means of determining the agreed (or required) protection that is attaching to specified individual data elements (fields and records) is addressed.

[47)] For a generic "information law" requirement from a LOV perspective, see further below Annex C (normative) *Integrated set of information lifecycle management (ILCM) principles in support of information law compliance*.

5.3.9 Privacy Protection Principle 9: Openness

The principle of "openness" pertains to the privacy protection requirement that any LET provider which collect and uses personal information shall be fully transparent in its use of personal information. This means that all of its policies and practices pertaining to the collection, use and management of any personal information shall be made readily and publicly available, free of charge, and via various means and media of communication.

Rule 028:
An LET provider shall have and make readily available to any Person[48] pecific information about its policies and practices pertaining to the management and interchange of personal information under its control.

In support of this principle the LET provider will have explicitly stated such information:

a) on its website; and,

b) have a policy in place to provide printed materials of this nature for free and upon request from anyone.

It is expected, that in support of this principle, the LET provider will have explicitly stated such information.

In addition, any agents and/or third parties that the LET provider may wish to involve in the learning transaction shall be fully cognizant of, able to comply with, and support the privacy protection policies and practices of the LET provider to which they are an agent or third party to.

Where protection scenarios are recorded for the purpose of Open-edi this principle is met by publishing the agreed scenario constraints, together with any external manual processes that have been used or providing references to them in an external source.

5.3.10 Principle 10: Individual Access

A key component of privacy protection requirements is that an individual learner shall be able to enquire of any LET provider (private or public sector) whether or not that LET provider has and maintain personal information about that individual learner anywhere in its record/information management systems. From a learning transaction and Open-edi perspective, this principle applies in particular to the DMAs in the IT systems of an LET provider.

It is anticipated that this principle will be enacted not through this standard but through laws and regulations of the applicable jurisdictional domain(s) pertaining to the learning transaction where an individual learner is a party to a learning transaction.

Rule 029:
An individual learner has the right to know whether or not an LET provider has personal information under its control[49] on or about that individual learner.

---

[48] "Person" is used here, instead of individual because other (potential) parties to a learning transaction, (e.g., organizations and public administrations) need to have access to an organization's privacy protection policies, practices and related information.

[49] The use of "under its control" covers the fact that the organization may engage agents, third parties, other parties to a learning transaction and thus provide them with personal information. However, the LET provider organization retains control of all its recorded information including personal information. This is already stated in Clause 6.4 *"Data component*" in ISO/IEC 15944-1:2010 and emphasized in Clause 6.4 *"Data component"* in ISO/IEC 15944-8:2011

Rule 030:
An LET provider, subject to privacy protection requirements, upon receiving a request from an individual learner shall inform that individual learner of the existence, use and disclosure of his or her personal information in any and all records management / information systems and in particular the DMAs of the IT systems which support the learning transactions of that LET provider.

Where this principle is implemented through Open-edi, the scenario, i.e. model, shall show the protection labels that are applied to the fields of data as part of the implementation of the scenario. It must be noted that this may be met by other means, such as the publishing of contact information for the point at which this information may be requested since there will be a need for the individual learner to prove they have the correct identity before a disclosure can be made.

Guideline 030G1:
Upon receiving a request of this nature, the LET provider may request the individual learner to provide personal information which will assist the LET provider in ascertaining whether or not it has under its control personal information on that individual learner. Personal information of this nature requested by the LET provider may include provision by the individual learner making the request for access (any combination of the following, in no particular order):

- ***one or more personae by which the individual learner may represent itself***[50)]
- ***the provision of a temporal period which may be applicable***
- ***the provision of one or more physical addresses which may be applicable;***
- ***the provision of one or more electronic addresses including telephone numbers, e-mails addresses, etc.;***
- ***the learning transaction identifier (LTI) pertaining to the learning transaction which led to the LET provider collecting and maintaining personal information about the individual learner making the request; and/or,***
- ***any other personal information, i.e. as data elements, which the LET provider receiving the request may require to ensure that its search for the existence of personal information relating to the requesting individual learner is as complete and thorough as possible.***

Rule 031:
Where an LET provider discovers that it has personal information on the individual learner who made the request, that individual learner shall be given full and complete access to any and all personal information which the LET provider maintains on that individual learner (unless there exist specified and referenced external constraints of the applicable jurisdictional domain(s) which prohibit access to one or more sets of such personal information).

The qualification on access to personal information in the above rule is necessary as ISO/IEC 29187-1 applies to both private and public LET providers as well as regulators.

The cost effective and efficient implementation of these privacy protection principles requires that the organization/public administration shall make publicly available its accessible fax or phone numbers, website URL, and where relevant, the name of its privacy protection officer (PPO) as to:

1) where and how an individual learner is able to obtain a complete record of its personal information; and,

2) how and where such personal information is used and interchanged with other parties to a learning transaction.

[50)] It is a fact that an individual has and uses many differing personae The organization receiving the request for "individual access" can only assume that the name that the individual uses is the same (or 95%+) the same as the one that it maintains in its IT systems. If not there may be no match. Thus, it is up to the individual to provide alternative personae to be used in any search/discovery.

The overall purpose of this principle is to ensure that the personal information which a Person retains on a specified individual learner is as accurate and complete at all times as possible. This means that where and whenever personal information on a particular individual learner which an LET provider has or retains for learning transactional reasons (or related legal "upon request" requirements) shall provide (be able to provide) a complete transcript of any and all personal information to the individual learner concerned about his/her personal information.

Guideline 031G1:
On the whole, based both on requirements of jurisdictional domains as well as "best practices" LET providers should ensure that:

1) **such information and documentation is available for free;**

2) **no costs are charged to an individual learner making a privacy protection request;**

3) **no costs are charged to the individual learner by the LET provider in providing the personal information it has on or about that individual learner;**

4) **such information and documentation is made available in the official language(s) of the jurisdictional domain in which the LET good, service, and/or right is being offered for sale;**

5) **such information and documentation is made available to individual learners in accordance with consumer protection and individual accessibility requirements.**

NOTE Users of this document shall refer to the ISO 639-2/T set of 3-alpha language codes to understand the use of codes representing official (and de facto) languages.

Rule 032:
Where an LET provider has and maintains personal information on the individual learner making the request for access to his/her personal information and such personal information does exist, the LET provider shall provide access to the personal information in a manner which is convenient to that individual learner.

Guideline 032G1:
While it is up to the LET provider and the individual learner concerned to agree on the most effective and efficient way to provide access to the personal information requested, it is up to the individual learner to decide as to what is the most convenient means for providing the personal identification identified.

Guidelines 032G2:
In cases where there is a difference of opinion between an LET provider and an individual learner about the accuracy of that individual's personal information held by the LET provider, it is advisable for the LET provider to maintain both (10 the personal information which the LET provider considers to be accurate; and (2) the personal information which the individual learner considers to be accurate.

These guidelines support a pragmatic approach in support of the fact that not all requesters use the Internet or have e-mail address or fax machines, etc. which support the provision of access to the identified personal information via attachments to an e-mail or via fax. That is, the LET provider may well have to send hardcopy or printout of the personal information requested to the individual learner.

5.3.11 Privacy Protection Principle 11: Challenging Compliance

Challenging compliance is a key privacy protection principle. It pertains to the right of an individual learner to question and thus challenge whether or not: (1) an LET provider has under its control (or maintains on behalf of other organizations) personal information on the individual learner; and, (2) if it does, that such personal information is accurate, timely, and relevant to the nature of the informed consent provided by that individual learner.

Depending on the privacy protection requirements of the applicable jurisdictional domain, an individual learner may have the right to:

a) challenge compliance directly with the LET provider to whom the challenge is directed;

b) direct such a challenge, (e.g., complaint) to a privacy or data protection commissioner/ombudsman as provide for in the jurisdictional domain; or,

c) various combinations of (a) or (b) above".

It is anticipated that this principle will be enacted not through this standard but through laws and regulations of the applicable jurisdictional domain(s) pertaining to learning transaction which involve an individual learner.

Rule 033:
An individual learner shall be able to challenge the accuracy and completeness of his or her personal information held by an LET provider with respect to a learning transaction (and/or part of a general client file) and have it amended or deleted as appropriate[51)]

It is to no one's benefit to maintain or make decisions on personal information which is not accurate or up-to-date. As such, one practical solution might be for the LET provider to maintain in its records both (1) the personal information which it considers to be accurate; and, (2) the personal information which the individual learner considers to be accurate. At the same time it may well be that the LET provider and the individual learner, in a learning transaction may not agree as to the accuracy of the personal information pertaining to that individual learner with respect to the learning transaction(s) entered into.

Rule 034:
An individual learner shall be able to challenge an LET provider concerning its compliance with the above eleven (11) privacy protection principles including assurance of privacy protection for any personal information that is interchanged with other organizations as agents or third parties (as well as secondary or derivative uses of personal information).

In effect, this means that any LET provider, to which privacy protection requirements apply, shall have:

a) in place the identification of a public contact, if other than that of its Privacy Protection Office (PPO), and physical address (e-mail optional) to which an individual learner can direct and challenge compliance of that LET provider with respect to personal information which that LET provider currents has on that individual learner (as well as secondary or derivative uses of that individual learner's personal information);
b) available a document which states clearly and explicitly the procedures the LET provider has in place to address a challenge to compliance with privacy protection requirements.

5.4 Requirement for tagging (or labelling) data elements in support of privacy protection requirements

The application of the general privacy protection principles, as stated in Clause 5.3 above, requires an LET provider to be able to identify and tag any and all personal information when it is created or collected in its IT systems. Such tagging is required enable an LET provider's compliance with specific privacy protection requirements. (It also assists the LET provider in meeting general ILCM requirements). An LET provider can do such tagging of sets of recorded information at the records (SRIs) level (e.g. client file level) down to the more granular data element level.

[51)] This rule requires an LET provider to track its master data and have data synchronization. These and related matters of traceability, including those pertaining to individuals are being addressed in the ISO/IEC 15944-9 "*Traceability Framework*" standard which is under development.

Rule 035
In order to ensure that a LET provider is able to identify quickly and accurately any and all personal information which it has, especially in its IT systems, it shall have in place policies and practices to tag all sets of recorded information (SRIs) which are personal information in nature and to do so at the appropriate level of granularity.

Further from data interchange perspective, among parties to a learning transaction, there are additional privacy protection requirements which apply.

Rule 036:
For SRI comprising personal information pertaining to a learning transaction, the following requirements apply from a data interchange, i.e., EDI, perspective there is the added need to ensure the provision of tag(s) to the personal information:

1) **shall not be communicated with other parties;**

2) **may be communicated to other parties but with restrictions; or,**

3) **may be communicated to other parties with no restrictions.**

Rule 037:
For a SRI comprising personal information pertaining to a learning transaction, the following requirements apply from a data interchange, i.e., EDI, perspective; namely, the need to ensure the provision of tag(s) to note that the personal information is subject to mandatory disclosure is:

1) **the actual information;**

2) **anonymous information that represents the actual information; or,**

3) **pseudonyms that represents the actual information.**

[THIS PAGE IS INTENTIONALLY LEFT BLANK]

6 Collaboration space and privacy protection[52])

6.1 Introduction

The concept of "collaboration space" is extremely useful in the context of privacy protection requirements and the eleven principles presented in Clause 5 above[53)] The construct of "collaboration space" provides a view which is independent of either the different but complementary perspectives of both the individual learner and the LET provider.

From an Open-edi perspective, the construct of "learning collaboration space" is a view that takes place outside of the internal control space of the individual learner and LET provider. A "collaboration space" is a methodology and tool which provides an independent view of the Persons involved in a learning transaction, i.e., in support of their activities and exchange of the recorded information they mutually exchange, the decision(s) taken, the commitment(s) made, etc.

In addition, the concept of "collaboration space works at both the level of:

a) internal constraints only;

b) also that of supporting external constraints of jurisdictional domains generally as well as those in particular of a "privacy protection" requirements nature.

6.2 Privacy collaboration space: Role of individual learner, LET provider and regulator[54)]

The focus of collaboration space is to be able to model the primary parties to a learning transaction. For modelling purposes, a learning transaction requires at least the roles of an "individual learner" and a LET provider, initially based on internal constraints only. However, since an individual learner is a primary party to a learning transaction involved in one or more sets of "external constraints" may apply. These are modelled through the role of a "regulator".

The concept of collaboration space, introduced and defined in ISO/IEC 15944-4, focuses on collaboration space from an internal constraints perspective only. ISO/IEC 15944-5 focuses on adding external constraints from the perspective of the requirements of jurisdictional domains[55)] They are modelled by adding a (1) regulator"; and, (2) the three sub-types of Person (as already introduced and provided for in Clause 6.2.7 in ISO/IEC 15944-1 titled "Person and external constraints "individual", "organization", and "public administration").

Where a Person is acting as (1) an individual; and, (2) in the role of a buyer the external constraints identified in Clause 5.3 in this standard may be required. Thus, when modeling a scenario, two possible approaches may be used. In the first it will be necessary to identify different scenario components in the model when addressing scenarios involving privacy from those not involving privacy. In the second the privacy constraints must be included in the model, with an option to switch them off for the scenarios where privacy requirements are absent. Either approach is valid.

---

52) In order to obtain a clear understanding of this Clause 6, users of this standard should familiarize themselves with Clauses 0.1-0.4 of ISO/IEC 15944-4 and Clauses 5.22 and 5.23 ISO/IEC 15944-5. Both are publicly and freely available standards.

53) The concept of collaboration space was first introduced in ISO/IEC 15944-4 *"Information technology – Business Operational View – Part 4: Business transaction scenarios – Accounting and economic ontology*". This ISO/IEC standard focused on "internal constraints" only. However, the concept of "collaboration space" has proved useful in presenting a "space" which is independent of parties to a commitment exchange, including those of learning transactions in nature.

54) This Clause is based on Clauses 5.2.2 and 5.2.3 in ISO/IEC 15944-5:2008.

55) See further ISO/IEC 15944-5:2008

There may therefore be more than one role being fulfilled by the regulator (or regulators) in the transaction, since the regulator may act to supervise that the information constraint(s) have been applied or may act to provide an anonymous or pseudonymous identity for one or more of the parties to the transaction (which may include themselves).

The regulator is the source of external constraints in a privacy collaboration space (PCS), defined as:

> ***privacy collaboration space (PCS)***
> *modelling or inclusion in an* ***Open-edi scenario*** *of a* ***collaboration space*** *involving an* ***individual*** *as the* ***buyer*** *in a potential or actualized* ***learning transaction*** *where the* ***buyer*** *is an* ***individual*** *and therefore privacy protection requirements apply to personal information of that individual provided in that* ***learning transaction***

The overall learning transaction being modelled (as a scenario or scenario component) involves (1) a "buyer" who is an individual; and, (2) the jurisdictional domain(s) involved have external constraints of a privacy protection nature.

Rule 038:
For any learning transaction (or part thereof) which involves external constraint(s) of a privacy protection nature, the Open-edi model shall include:

1) **the Person in the role of buyer as an individual;**
2) **the role of the regulator(s) representing the source of privacy protection requirements for modelling as part of a scenario and scenario components;**
3) **the role of the regulator(s) providing proof of identity of the individual without necessarily disclosing the actual identity of the individual.**

This is illustrated in Figure 3 below (as adapted from Figure 5 ISO/IEC 15944-5).

It is noted that in some learning transactions the seller as well as the buyer may be both making use of an agent or a third party supplier for the purpose(s) of concluding a learning transaction.

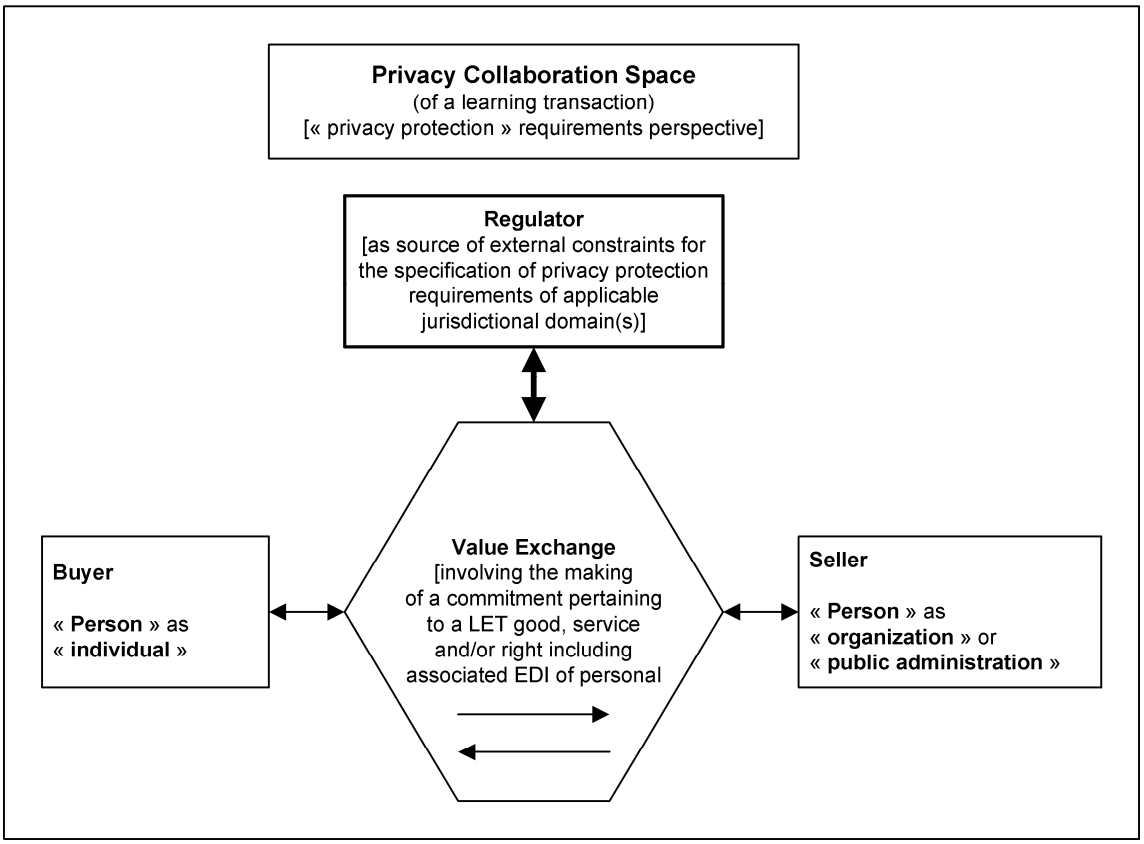

Figure 3 — Privacy collaboration space (of a learning transaction) including the role of a regulator

6.3 Learning collaboration space (of a learning transaction)

The last point to be made here is that a learning transaction between an “individual learning” and a “LET provider” needs to be viewed not only from the perspective of each of these two parties but one that is common to both, i.e. as an independent view of their common “collaboration space”

Figure 4 below is adapted from Figure 5 in ISO/IEC 15944-5 and Figure 3 in ISO/IEC 15944-8**.**

Figure 4 below is adapted from Figure 3 above (as well as Figure 5 in ISO/IEC 15944-5 and Figure 3 in ISO/IEC 15944-8).

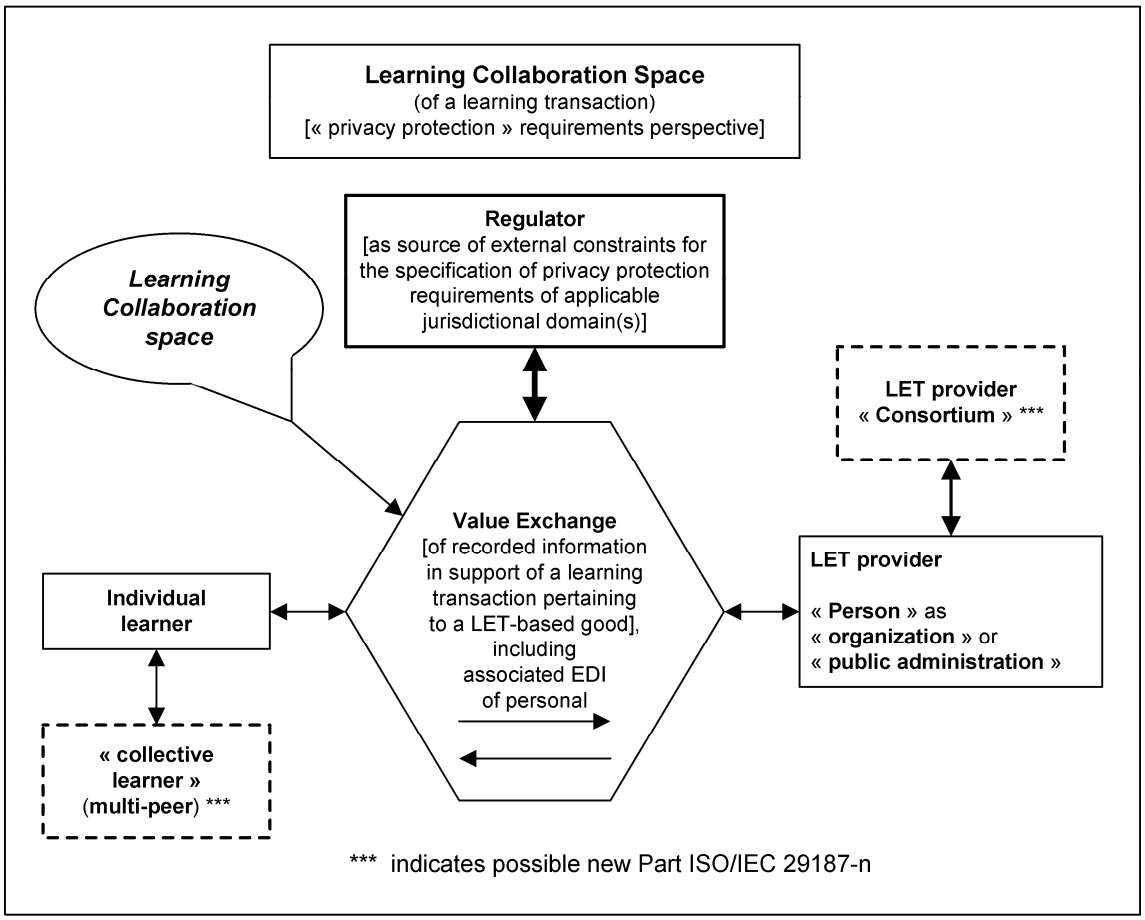

Figure 4 — Learning collaboration space (of a learning transaction) including the role of a regulator (as well as "collective learner' and/or LET provider "consortium(s)"

7 Public policy requirements of jurisdictional domains

7.1 Introduction

The purpose of Clause 7 is to place privacy protection in the context of public policy requirements, i.e., the overall legal and regulatory requirements which apply to an individual learner as a “buyer” generically in a learning transaction in an ITLET context. The focus here is the fact that when the buyer is an individual learner then the (legal) rights, which an individual has, must be supported and modelled.

Clause 6.3 in ISOIEC 15944-5 sets out the overall approach and key rules. They are summarized here, and expanded with respect to the privacy protection perspective and in an ITLET context.

7.2 Jurisdictional domains and public policy requirements

Increasingly jurisdictional domains require those providing a LET good, service and/or right in making such offers, and those executing resulting (electronic) learning transactions, to comply with requirements expressed as rights pertaining to natural persons in their role as individual learners[56)] Clause 0.2 and Figure 3 in ISO/IEC 15944-1:2010 identified these as "public policy" requirements. “Public policy” subsequently has already been defined in ISO/IEC 15944-5:2008. {For text of the definition for `public policy``, see above Clause 3}

Clause 6.2.8 in ISO/IEC 15944-1:2010 titled "Person and external constraints: constraints: consumer and vendor" introduced "consumer protection" as a minimum external constraint which needs to be taken into account in modelling learning transactions, involving an individual as “buyer”, doing so in a limited manner.

There are other external constraints of a "public policy" nature which need to be taken into account in modelling learning transactions. These include “individual accessibility[57)], human rights, etc.[58)]

This Clause 7.2 focuses on some of the most basic categories of public policy as external constraints that need to be taken into account in modelling (electronic) learning transactions which involve "individuals" as "learners". Those already identified include:

1) privacy protection

2) consumer protection;

3) individual accessibility; and,

4) human rights.

[56)] Note: A natural person, a human being, acting in the role of “seller” is deemed to be an “organization” (as per ISO/IEC 6523 definition and common (legal) practices.

[57)] With respect to “individual accessibility”, JTC1/SC376/WG7 is currently completing development work on ISO/IEC 20016-1 “ITLET - Language accessibility and human interface equivalencies (HIEs) in e-learning applications – Part 1: Framework and reference model for semantic interoperability”.

[58)] As per Annex B "Learning transaction model: Classes of constraints below these form part of the category of "External Constraints: Public Administration" (as identified in Figure 8 in ISO/IEC 15944-1).

This is illustrated in Figure 5 below

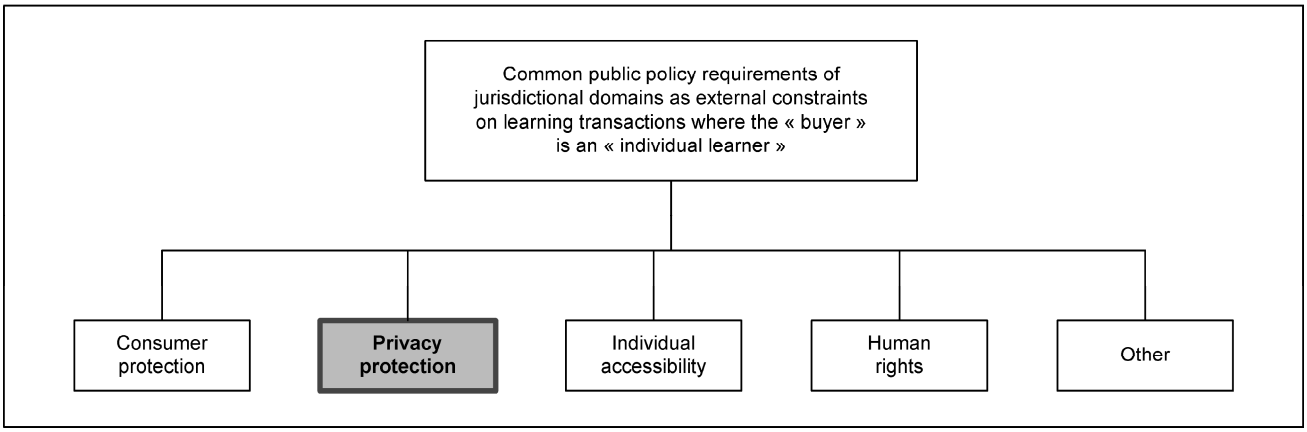

Figure 5 — Common public policy requirements, i.e., external constraints, applying to a learning transaction where the "buyer" is an "individual learner"

The following four sub-clauses summarize the minimal external constraints of this nature in a very simple form. It is outside the scope of this part of ISO/IEC 29187 to address and specify detailed external constraints on a learning transaction of the nature of "consumer protection", "individual accessibility", etc., in specific detail.

7.2.1 Privacy protection

In modelling (electronic) learning transactions, a common minimum external constraint that needs to be taken into account is that commonly referred to as privacy protection requirements. In this standard, the term "privacy protection" is used to identify the public policy requirements addressing both of these topics. Privacy protection requirements apply to any learning transaction in which an individual is a "buyer".

Rule 039:
A common set of external constraints of a jurisdictional domain on a learning transaction, where the buyer is an individual learner, are those of a privacy protection nature.

Rule 040:
Where the buyer in a learning transaction is an individual, external constraints of a privacy protection nature of jurisdictional domains apply and shall be supported.

The focus of this sub-Clause is to specify key rules which are applied to any Person in the role of a seller, i.e., as an organization and public administration, who offers or provides a LET good, service, and/or right to prospective buyers as individual learners.

It is noted that from a LET provider perspective, privacy protection requirements can be summarized as maintaining recorded information about an identifiable individual learner which is as timely, accurate, and relevant as possible, is used only for its original purpose and not for any other purpose (unless consented to by the individual concerned), and that any such recorded information which does not meet these requirements is expunged, unless there are other external constraints of a jurisdictional domain nature which override such privacy protection requirements, (e.g., law enforcement, national security, etc.). The key primitive privacy protection principles which apply here are stated above in Clause 5.

The application and implementation of this rule has as a logical consequence that any Person offering a LET good, service and/or right as a seller in a learning transaction i.e., including a LET provider in a learning transaction shall explicitly state that the good, services and/or right, as a goal in a learning transaction, is or is not offered to an individual learner.

Rule 041:
Any Person offering a LET good, service, and/or right as a LET provider shall explicitly state whether or not the same is available for purchase by any Person in its role as an "individual".

For example, certain goods, services and/or rights may be proscribed from being offered for sale, and thus not sold, to an individual.

Rule 042:
Where the buyer in a learning transaction is an individual, external constraint of a privacy protection nature of jurisdictional domains apply and shall be supported.

Rule 043:
Any Person offering a LET good, service, and/or right as a seller, in a learning transaction, which can be obtained by an individual as buyer, shall have in place and implemented an auditable privacy polity of the nature stated in Clause 5 above.

Rule 044:
A LET provider shall ascertain, at the identification phase in the process leading to a learning transaction, whether or not the buyer is an individual (not someone as organization Person buying on behalf of an organization or public administration)[59)]

Guideline 044G1:
Where a jurisdictional domain differentiates in criteria for privacy protection with respect to a natural person in its role as an "individual" or an "organization Person," this needs to be specified.Guideline 044G2:

Where a jurisdictional domain has privacy protection requirements as a set of external constraints which are applicable to a specific sector (public versus private, per industry sector, etc.), or type of learning transaction, this shall to be specified.

7.2.2 Consumer protection

When an individual learner is requested or required to pay a fee of whatever amount associated with the completion of learning transaction being provided in relation to a learning transaction, public policy requirements of a consumer protection requirements (will likely) apply. It is noted that many external constraints pertaining to personal information of an individual are similar in nature from both privacy protection and consumer protection requirements.

Rule 045:
A common set of external constraints of a jurisdictional domain on a learning transaction, where the buyer is an individual learner, are those of a consumer protection nature[60)] As such, any learning transaction involving an "individual learner" in the role of buyer shall be structured to be able to support applicable "consumer protection" requirements.

"Consumer" and "vendor" have already been defined in ISO/IEC 15944-1:2010 and "consumer protection" in ISO/IEC 15944-5:2008. {For text of definitions for these concepts, see above Clause 3.023, 3.160. and 3.023, respectively for the text of the definitions}.

[59)] See further below Clause 10 "Process component of a learning transaction". This Clause in turn is based on more detailed normative text found in n ISO/IEC 15944-1:2010 Clauses 6.2 "Rules governing Person"; Clause 6.3 "Rules governing the process component"; and, Clause 6.4 "Rules governing the data component" as well as its Annex F (informative) "*Business transaction model: process component"*

[60)] This is a restatement of "Rule 38" in ISO/IEC 15944-1:2010.

Rule 046:
Where the buyer is a learner, the LET provider shall ascertain that the learner has the age qualification required by the jurisdictional domain to be able to be involved in and make commitments pertaining to the LET good, service and/or right being offered in the proposed learning transaction

Guideline 046G1
A LET provider shall take the required precautions to ensure that it does not communicate inappropriate information, engage in monetary transactions, or in the making of any commitments with those who do not have the capacity to engage in them such as minors, (without the verifiable consent of their parents or guardians), or those without legal capacity, as may be required by the jurisdictional domain of the buyer.

This rule and guideline captures common consumer protection requirements pertaining to sales in general as well as to particular goods or services to children and minors who may not have the legal capacity to engage in such actions in the jurisdictional domain of the buyer (and/or seller).

Rule 047:
A LET provider shall ensure that where it intends to sell a LET good, service and/or right to a buyer as an individual that consumer protection requirements of the applicable jurisdictional domain of the buyer are supported.

These consumer protection requirements include the provision of “complete” information, the use of language of the individual, terms of contract formation and fulfilment, privacy of the on-line information, security of the personal information and payment, procedures for redress, stop to unsolicited e-mail, etc. Note that the place of delivery may affect the ability of the individual learner and LET provider to act.

7.2.3 Individual accessibility

An external constraint of a public policy nature that shall to be taken into account by a LET provider categorized is individual accessibility[61)] requirements in the form of either (1) rights of individuals in their use of information technologies at the human interface; and/or (2) those providing LET goods or services do discriminate against or prevent participation by “non-typical” users, i.e., those persons with an impairment or disability of some kind, who require some form of adaptive semantics and technologies to participate in a learning transaction, viz. “individual accessibility”. Here "individual accessibility" pertains to ensuring that LET goods or services being provided in (electronic) learning transactions can be used by people with impairments or disabilities.

Here disabilities can be of either a functional or cognitive nature.

61) “Individual accessibility” has already been defined in ISOIEC 15944-5:2008. See above Clause 3.051 for the text of this definition.

It is noted that language and cognitive disabilities are very difficult to specify and thus model as human interface requirements[62] but often it is possible to do so. They include mental retardation, lack of short term memory, dyslexia, dyscalculia, dysgraphia, auditory and perceptual disabilities, cognitive disorganization, and visual perceptual disabilities.[63] Nevertheless, unless a human disability (ies) of an individual is of the nature where the jurisdictional domain considers or declares the individual to be "incompetent", i.e., not able to make a commitment as a party to a learning transaction, from an external constraints perspective, there is a need to be able to support human accessibility requirements. This includes the provision of “alternate formats”, i.e. the provision of the semantics of the recorded information is in a representation form, which the individual as (prospective) buyer is able to understand in an unambiguous manner in order to be able to decide whether or not to make the commitment(s) associated with the actualization of a learning transaction.

Rule 048:
In the development of human interface equivalents (HIEs) for an ID code[64] or a semantic identifier, these must also include those HIEs of a nature to ensure individual accessibility[65]

7.2.4 Human rights

The three public policy requirements identified above apply to Persons in their role as an individual learner engaged as a "buyer" (or "consumer") in a learning transaction. There are other public policy requirements which may need to be supported of a "human rights" nature in modelling a learning transaction. Here in the context of "cultural adaptability" as the third strategic direction of ISO/IEC JTC1 for its standards development[66] other public policy requirements which may need to be incorporated into the specification and re-use of business objects include:

1) the UN "Universal Declaration of Human Rights" (1948);

2) the UN "Universal Declaration of Rights of Persons belonging to National or Ethnic, Religious and Linguistic Minorities";

---

[62] Annex A in ISO/IEC 5218:2004 “*Codes representing the human sexes”* titled “ *Annex A (Informative) — Codes for the representation of the human sexes supporting (linguistic) cultural adaptability/Annexe A (Informative) — Codes de représentation des sexes humains supportant l’adaptabilité culturelle (linguistique)*” provides an example.

[63] See further the US National Institute of Neurological Disorders and Stroke resources on dyslexia at <http://www.ninds.nkh.gov/healthandmedical/disorders/dyslexiadoc.htm. See also the "*IMS Guidelines for Developing Accessible Learning Applications*", Version 1.0 White Paper, 2002-06-22 (publicly available via http://www.ims.org) as well as other IMS documents containing very useful information and IT systems specifications for individual accessibility requirements from an “ITLET” perspective. {http://imsglobal.org/accessibility}. This IMS work has been progressed as a multipart international standard through JTC1/SC36 as ISO/IEC, 24751 Individualized *Adaptability and Accessibility in e-Learning, Education and Training*, of which the first three parts are already published, IS standards.

Part 1: Framework and Reference Model

Part 2: “AccessForAll” Personal Needs and Preferences for Digital Delivery”

Part 3 : “AccessForAll” Digital Resource Description”

Note should also be taken here of the development by ISO/IEC JTC1/SC36 of the multipart ISO/IEC 20016 standard titled *ITLET - Language Accessibility and Human Interface Equivalencies (HIEs) in e-Learning applications: Principles, Rules, and Attributes*

Documentation on this standards development work is available at the JTC1/SC36 site at <http://www.jtc1sc36.org >

[64] The development of Part 10 “Coded domains” of ISO/IEC 15944 incorporates the ability to support individual accessibility requirements.

[65] Table 1 in Annex A of ISO/IEC 5218:2004 provides an example of an IT-enabled approach to supporting individual accessibility. It has been reproduced in Annex D. ISO/IEC 15944-7 is structured to be able to support individual accessibility requirements, i.e. through the development of additional normative Annexes in support of the same.

[66] The other two strategic directions of ISO/IEC JTC1 for standards development are "portability" and "interoperability".

3) the UN "Universal Declaration of Cultural Diversity" (Paris, November, 2001);

4) international Covenant on Economic, Social and Cultural Rights 1966, United Nations (UN); and,

5) UN Convention on the Rights of Disable Persons (2006).

7.2.5 Privacy as a right of an "individual" and not right of an organization or public administration[67)]

Rule 049:
Privacy protection requirements apply only to a natural person, i.e., human being, acting in the role of an individual.

Organizations or public administration do not normally have any common law or statute law right" to privacy protection because public policy does not consider them to require statutory protection. They by definition are "legal persons" and not "natural persons". {See further Figure 16 Clause 6.2.7 and Figure E.19 Annex E in ISO/IEC 15944-1 as well as associated rules and text}

7.2.6 Need to differentiate between "privacy protection" and "confidentiality", "security", etc.

An organization or public administration may introduce and maintain requirements of a "confidentiality" or "secrecy" nature with respect to an identified set(s) of recorded information (included as semantic components or information bundles. among participating parties to a learning transaction. However, requirements of a "confidentiality" and "secrecy" nature would need to be identified, negotiated and agreed to as part of contract formation pertaining to a learning transaction are not in the scope of this standard, although similar methods may be used in modelling as those for privacy.

This is part of the broader field referred to as of information security labelling in ISO/IEC 27002:2005.[68)] Information is labelled according to the overall protection constraints that are to be applied to it. Information that is confidential is generally labelled so that supporting FSV mechanisms are able to determine if the information is being accessed by an entity that is properly authorized. Privacy protection labels (as shown in Section 5) are used to determine what subsequent use (if any) the authorized entity may make of the information that is labelled. So, at a simple level, the recipient of information that is confidential is not limited in the subsequent use that they make of that information, whilst the recipient of information that has privacy is explicitly constrained as to the subsequent use. As such, privacy protection labelling is separate and independent of confidentiality labelling although both make use of similar supporting mechanisms, (e.g., as part of LET-FSV services).

---

67) In the preparation of this Part 1 of ISO/IEC 29187 no applicable law or regulation was identified in jurisdictional domains which state that an organization has an explicit right to "privacy protection" as an organization.

68) See further ISO/IEC 27002:2005 *Information technology -- Security techniques -- Code of practice for information security management.* In addition, the ITU-T has standards development activities pertaining to privacy protection and use of ICT, i.e., from a FSV perspective. Similar, ISO/IEC JTC1 has several standard development committees addressing privacy protection issues from both a BOV and FSV perspective, (e.g., JTC1/SC31 and SC37) or from an FSV perspective, (e.g., ISO/IEC JTC1/SC27)

8 Principles and rules governing the establishment, management and use of identities of an individual (and "individual learner")[69)]

8.1 Introduction

It is a very common practice that an individual learner is assigned an identifier by a LET provider within the context of that learning transaction specifically or generally where the individual learner is enrolled in a study program at whatever level. {With respect to the establishment of a Learning Transaction Identifier (LTI) see further below Clause 11.2}

Since an individual learner can participate in many different learning transactions (and other commitment exchanges), there will have many different combinations of name representations, a.k.a., as "persona," and identifiers as identities. Thus, there is the need for a systematic approach to the management of identities. Published work seems to focus on the Functional Services View (FSV) aspects, i.e., the "How to" without first defining the business operational view (BOV) requirements, i.e., the "WHATs". In this standard, this is the Learning Operational View (LOV). This section focuses on the "WHATs". In addition to addressing the establishment, management, and use of identities of an individual based on external constraints, this section focuses on supporting external constraints of a privacy protection nature.

The concept of "identity management", or better phrased "management of identity(ies)" of an entity, is viewed differently from various perspectives. Its widest perspective is that at the entity, i.e., pertaining to any person, object, event, idea, process, etc. {See further Clause 3.44 definition of entity} Within an Open-edi context, a differentiation is made between "Person" and "non-Person". Generic issues pertaining to the need for unambiguous identification of entities in (electronic) learning transaction are already identified and resolved in ISO standards. The focus of the multipart ISO/IEC 29187 standard Is the unambiguous identification in a learning transaction of Persons (as individual learners) [70)] only and thus not objects[71)] events, processes, etc. [72)] {See further Annex C "Unambiguous identification of entities in (electronic) learning transaction" in ISO/IEC 15944-1:2010 (2nd edition)[73)] The focus of ISO/IEC 20187-1 with respect to "management of identities" is not on Persons in general but that of an individual learner (as a sub-type of Person) in particular.[74)] As such, this ISO/IEC 29187-1 sets out the principles and rules governing the establishment, management, and use of identities of an individual which are to:

---

69) See further Annex E below titled *(Normative) Key existing concepts and definitions applicable to the establishment, management, and use of identities of a single individual*

70) In support of this approach ISO/IEC 21987-1 also contains an Annex D titled "Existing standards for the unambiguous identification of Persons in learning transactions (organizations and individuals) and some common policy and implementation considerations".

71) ISO, IEC and ITU standards for the unambiguous identification of objects (including tokens) are many. Standards here developed and maintained by ISO/IEC JTC1/SC17 "Identification cards" and those by JTC1/SC31 *"Automatic identification and data capture techniques*" and the resulting ubiquitous use of bar codes are the most commonly known. In addition, various industry sectors also served by one or more international standard of registration and identification schemas and assignment of unique identifiers for each unique objects, (which in turn usually has many clones with the same ID as result of mass manufacturing, publishing, etc.).

72) Users of this standard should be aware of the fact that many of the issues pertaining to "identity management" with respect to a Person (natural or legal) are also identified and addressed in ISO/IEC 15944-1 as well as in the Parts 2, 4, 5, and 8 of this multipart ISO/IEC 15944 standard.

73) A guiding principle in the development of the multipart ISO/IEC 15944 standard is that it is structured to be able to support the need to differentiate among the three sub-types of "Person" namely "individual", "organization" and "public administration".

74) Here this Part 1 of ISO/IEC 29187 maximizes the use of other ISO and IEC standards as well as Referenced Specifications relevant to the privacy protection requirements in a BOV (and not FSV) context.

1) based on those which already apply to a Person in a generic manner, as already found in the following normative Clauses of ISO/IEC 15944-1,

   Clause 6.1.4 – Learning transaction: unambiguous identification of entities

   Clause 6.2.2 – Person, personae identification, and Person signature; and,

   Clause 6.2.3 – Person, identity and authentication; and,

2) apply the Clause 5 Privacy Protection principles of this ISO/IEC 29187-1 to an "individual" as a defined sub-type of "Person".

8.2 Rules governing the establishment of personae, identifiers and signatures of an individual

This sub-clause and its rules:

1) applies the existing rules as well as associated concepts and their definitions of ISO/IEC 15944-1 pertaining to Person and adapts them to ISO/IEC 29187-1 based on the eleven privacy protection principles (set out in Clause 5 above) and, doing so in an ITLET context and from a collaboration space perspectives;

2) includes added rules which apply where an individual is a buyer, i.e. as individual learner, in a learning transaction; and,

3) takes an integrated approach.The rules which follow below (as well as those found in Clause 8.5 below),

The rules which follow below (as well as those found in Clause 8.5 below),

1) support this integrated approach and support the real world conditions noted above;

2) support the fact that it is up to a Registration Authority to decide, and therefore accept due liability (which must be made clear to the parties) for the correctness of their assertion, based on applicable criteria in the jurisdictional domain of that Registration Authority, i.e., applicable set(s) of internal constraints; whether or not to register an individual learner as a member, of a coded domain, and if so assign an ID code, to that individual together with any qualifications as to the liability taken by the Registration Authority as to the provenance they grant individuals.

   It is noted that a Registration Authority, i.e. an organization or public administration, may be responsible for the management of more than one registration schema (RS). Consequently, the "same" real world individual may or may not be eligible to become a member of the different RSs being managed by a single RA.

   For example, from an external constraints perspective, a single organization as a Person, i.e., as an incorporated (legal) entity with the associated accepted legal name(s[75)] as part of the incorporation, and also may use other names in conducting its learning transactions including trademarks.

For this standard, a Registration Authority is an organization or public administration that is responsible for the management of one or more registration schema (RS). Consequently, the "same" real world individual may or may not be eligible to become a member of the different RSs being managed by a single RA. For example, an individual learner may be qualified to enrol in one faculty in a university but not in another.

A Person has one or more persona (and associated identifier(s) with each) resulting in one or more Person identities (Pi) depending on the status and role qualification requirements of the Person to able to be

[75)] Where a jurisdictional domain has more than one official language, "legal" person may well have more than one official name, i.e. in each of those official languages. This is most often the case with public administrations.

registered for and obtain the resulting assignment of a unique identifier. The same approach also applies to an individual learner obtaining a unique identifier from a RA.

Rule 050:
The primary set of generic principles and rules, as well as associated concepts and their definitions governing the creation, recognition, use, management of identities of a Person as stated in Clauses 6.1.4,and 6.2.2 of ISO/IEC 15944-1, apply to this Clause 8.3 of ISO/IEC 29187-1.

The interworking of these generic rules in Clause 6.2.2 of ISO/IOEC 15944-1, results in a variety of combinations of linkages currently existing among personae, identifications, and Person signatures for the same single real world individual. This is illustrated in Figure"7" below, (which integrates and is a composite of figures 9, 10 and 11 as found in Clause 6.2.2. ISO/IEC 15944-1). (In Figure 6, different fonts and representations are used for: "Person signature" to recognize the wide variety in forms and information technologies used to capture "Person signatures[76)] " i.e., in this case of an individual.)

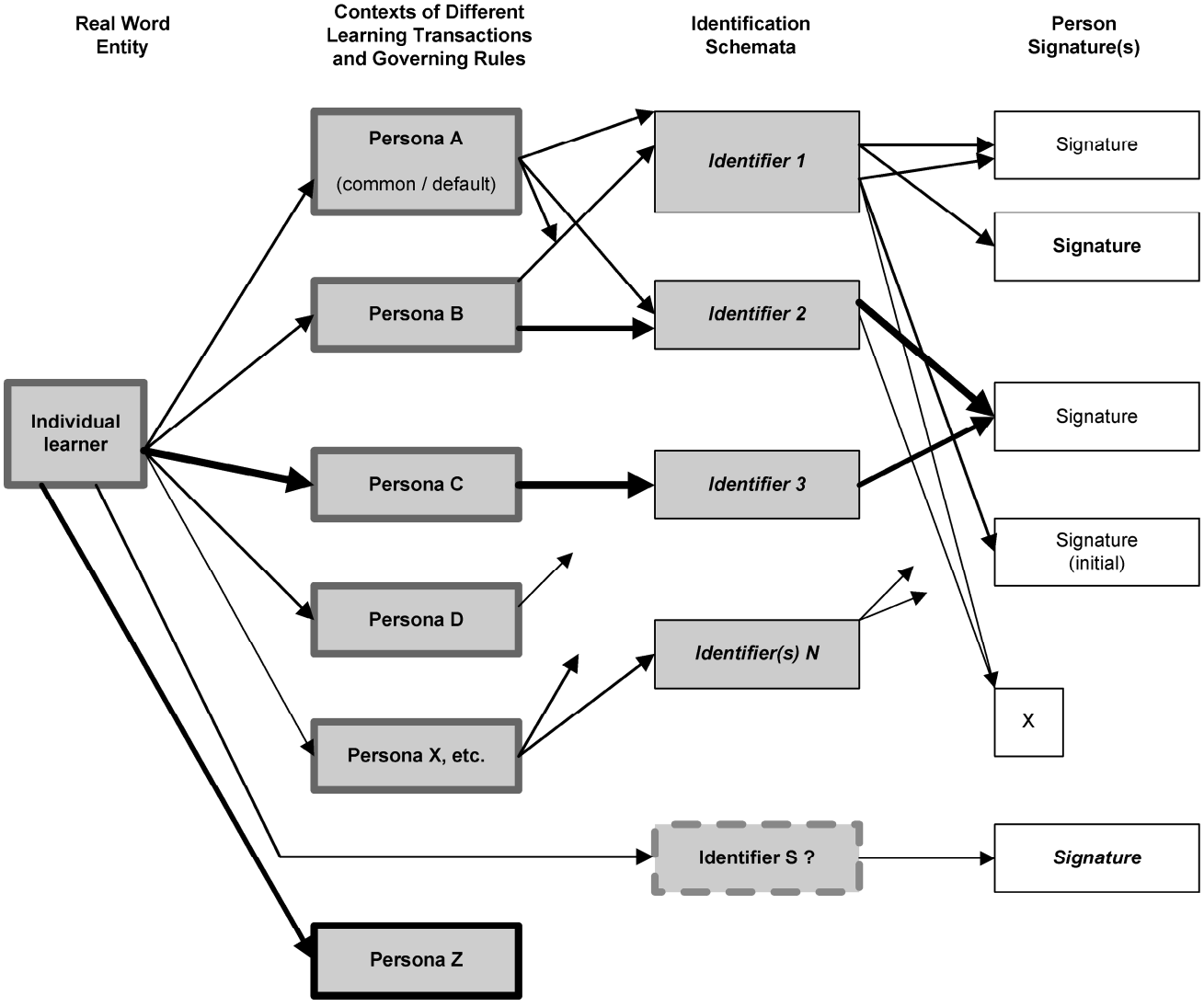

Figure 6 — Illustration of relationships of links of a (real world) individual learner to (its) persona (e) to identification schemas and resulting identifiers to associated Person signatures — in the context of different learning transactions and governing rules

[76)] One should note that the definition of signature and rules in Clause 6.2.2 of ISO/IEC 15994-1 allow for the use of different signature forms and may be created by different processes, ranging from physical to advanced biometrics

This includes and supports the following real world conditions[77)]

1) an individual learner during its lifetime may have many multiple different personae, i.e. names, depending on the roles that it has or qualifies for.

   For some of these personae, the individual may assign or adopt for itself while other personae used may be qualified as to whether or not they may be used as a persona in the identification schema of a Registration Authority (based on the rules governing the formation, representation and use of names of registrants of that Registration Authority). For instance, people on the point of marriage may create personae not previously in existence as well as retain previous personae;

   For example, at the time of marriage an individual may acquire and use a new (legal) persona. Similarly, based on the rules and criteria of the applicable Registration Authority) the persona of an individual as written on its birth certificate may not be the same as stated in an immigration record, a passport, a drivers licence, a social insurance or health insurance card, etc. Consequently, an individual may and will have multiple legally recognized names (LRNs), recognized individual names (RINs), recognized individual identities (riis) at the same time (and so used in various learning transactions).

2) unless prescribed by a specific external constraint, an individual is free to use any "persona" to represent itself[78)]

3) an individual during its lifetime will have and use multiple different identifiers, i.e. individual identities depending on the roles that it has, qualifies for, or is assigned by nature of its status or actions;

   It is likely that an individual identity (ii) established by an individual in the context of a specific Registration Authority (RA) may have limited use as decided by the individual and/or Registration Authority

   Examples include a persona which an individual assign to itself and is one which also serves as an identifier such as an e-mail address (on a hotmail or gmail account, Facebook, Twitter, as an "avatar", etc.

4) an individual during its lifetime often has and does use different forms or representation of its Person signature.

   Common examples here include the use by an individual of a "short name signature, the use of an initial, the use of a first name and surname only, the use of a initial and surname only and other signature forms whether physical or electronic in nature, (e.g. personal seals, symbols, document embossings, stampings, etc.).

5) only a specific persona of an individual may be eligible for use in an identification schema of a Registration authority before an associated identifier can be assigned by the RA.

   This is illustrated with "persona C" (e.g., an individual shall use the persona as stated in its birth certificate, landed immigrant, or residence permit document (or its accepted Latin-1 alphabet equivalent where the IT systems of identification schema of the Registration Authority supports only the Latin-1 character subset of ISO/IEC 10646);

[77)] It is also noted that an assigned identifier, i.e., once assigned by the Source Authority, can be assigned without the use of a "persona", (e.g., as an "anonymous ID). Here in Figure 7, the use of "Identifier S". In addition, identifier "S" represents an identifier being assigned to an individual without a persona, (e.g., an anonymous ID usually associated in its use with an additional password or code which replaces (in part) the use of a persona.

[78)] The use of a persona by an individual for fraudulent purposes, a.k.a. "personation", is a criminal offence in (most) jurisdictional domains.

6) An individual in qualifying for a new role and becoming a member of a registration schema of a Registration Authority may well be assigned a “new persona” in addition to the associated identifier.

The fact of an individual being assigned a “new” persona is a not infrequent occurrence where the movement of individuals from one jurisdictional domain to another resulting in the individual obtaining a new or different civil status in a jurisdictional domain. For example, the written form of the persona of the individual who moves to another jurisdictional domain as immigrant, resident, refugee, etc., may well be in a language and or writing system which is different from or not supported in the new jurisdictional domain. This is evidence in the resulting documents issued as proof of civil status.

This is quite often the case with students who transfer from a jurisdictional domain which uses non-Latin character sets to enrol in a school or university which uses the Latin-1 character set for name representation, including the persona of the individual learner.

7) the Person signature form used by the individual at the time the persona was registered and the identifier assigned shall be same to be used in any and all transactions (and interactions) of that individual when using the identifier assigned by that Registration Authority.

Common examples here include requirements of this nature in the financial services and banking sector, where the signature form of the individual when first registered by banks or financial service, where the signature form of the individual when first registered by banks and financial services, as so recorded manually (on a signature card maintained by the issuer or on the back of the card issued) or electronically by that registration authority must match and continue to match the signature form used by the individual when using that specific identifier for a particular purpose;

8) a persona used by an individual may well not be linked to any identification schema and thus any identifier, i.e., ID code in a registration schema of an RA.

This is illustrated by the box representing “persona Z”.

9) an individual may be registered in a registration schema (RS) of a Registration Authority (RA) by its resulting identifier and without a persona being maintained.

This is illustrated by the box representing “identifier S”. An example here is an individual having a numbered account with a bank which does not require the individual’s persona for its use but other (non-) personal information which is deemed to be sufficient to absolutely identify the persona for the purposes of effecting monetary or transactions which are “monetized|” in one form or another..

10) in most cases the identifier assigned by the Source Authority is of the nature of a composite identifier

The construction, maintenance and use of a composite identifier is based on a set of rules, and the identifier assigned is therefore parse-able.

For example, the identifier on one’s credit/debit card or any other card issued based on the use of the ISO/IEC 7812 is a composite identifier[79)] as is any organization identifier based on ISO/IEC 6523[80)]

---

79) For information on how this composite identifier is composed and related summary information, see ISO/IEC 15944-1:2010, Clause D.4.2.3 titled *“(Global) unambiguous identification of “buyers” and “sellers” – ISO/IEC 7812”*

80) For information on how this composite identifier is composed and related summary information, see ISO/IEC 15944-1:2010 Clause D.4.2.2 titled *(Global) unambiguous identification of “organizations” – ISO/IEC 6523”.* Here one notes that IANA is registered under ISO/IEC 6523 with its international code designation (IDC) being “0090” for the Internet IP addressing, i.e., internet IP addresses, like international telephone numbers are composite identifiers (and thus parse-able which facilitates their use in IT systems.

With respect to the identification schema and the creation of identifiers, i.e. as the ID codes in the coded domain, of that identification schema, it is noted that:

1) it is the Registration Authority (RA) which assigns the identifier when the individual meets the stated criteria and is registered as a member of that coded domain(s) of the RA;

2) the status, eligibility and/or qualifications of the individual may result in:

   a) "mandatory[81)] registration with a particular RA, i.e. often due to a specified external constraints of a jurisdictional domain; or,

   b) "voluntary" registration by the individual with an RA can be based on a requirement of an internal constraints nature by the seller; i.e. that based on internal constraints of the seller[82)] or those based on external constraints of a regulator.[83)]

Rule 051:
An individual may have and often does have multiple different personae, i.e., names in the lifetime of that individual. More than one persona may be valid in one or more jurisdictional domains at the same time.

It is a fact, that during the course of the life of an individual, that an individual most likely has and uses more than one personae in its lifetime. Significant factors here include:

1) mobility and migration of individuals from one jurisdictional domain to another including the fact that this involves the use of different official languages. The most common example here is that the jurisdictional domain in which the individual is born has a language and/or writing system which is different from the jurisdictional domain into which the individual has immigrated to (or becomes a legal resident or citizen of);

2) that through marriage (or similar change in civil status), the individual (legally) obtains or uses a persona different from its "birth certificate persona";

3) the fact that the individual decides to use a variant (new) persona which is different than that stated on its birth certificate and uses this new persona has become its default "persona" which in turn may become a RIN.;

4) the fact that an individual as a child (or minor) may be subject to a divorce of its parents and thus obtain, i.e., be assigned, a new surname;

5) the fact that an individual may request and receive a legal change of name in the applicable jurisdictional domain;

6) it is recognized that an individual in using ICT and in particular the Internet may well represent itself with a persona which is quite different from any of its personae used in the "physical" world.

---

81) Primary examples here are the mandatory requirement of registration of an individual at birth, registration of marriage, need to have a passport or similar travel document for crossing international boundaries, etc. Often these are linked to permitted methods of payment (e.g. use by the buyer of a credit or debit card only for payment in a learning transaction.

82) Often these are linked to permitted methods of payment (e.g. use by the buyer of a credit or debit card only for payment in a learning transaction.

83) Examples here include an individual qualifying for a license of some kind (e.g. driver's license, professional license for a doctor, engineer, architect, etc.)

Rule 052:
An individual may have, and often has, one or more recognized individual names (RINs) including two or more simultaneously existing RINs and thus more than one recognized individual identity (rii).

A recognized individual name is any personae associated with a role of an individual which is recognized as having legal status, i.e., if a legally recognized name (LRN) and is so recognized in a jurisdictional domain as accepted or assigned in compliance with the rules applicable of the registration schema of that jurisdictional domain as governing the coded domain of which the RIN is a member. Associated with a registered individual name is (usually) a registration number of the document attesting to the RIN having legal status of some kind.

Common examples of RINs with directly associated rii's include:

1) a birth certificate name and birth registration number as issued by the jurisdictional domain in which the birth of the individual is registered;

2) a marriage certificate name and marriage registration number as issued by the jurisdictional domain in which the marriage of the individual is registered. Note: an individual may have more than one married name but (normally) only one is valid at any one time.

3) a passport name and passport registration number as issued by the jurisdictional domain which issued the passport based on the applicable eligibility rules for that coded domain.

4) Note: An individual may have more than one type of passport (depending on its role) as well as more than one passport issued by different jurisdictional domains (depending on the rules of those jurisdictional domains). Some individuals may hold multiple passports both in their own apparent names and also different apparent names;

5) a medical or health name and card registration number as issued by the jurisdictional domain which issues the card based on applicable eligibility rules;

6) a driver's license and registration number as issued by a jurisdictional domain based on the individual qualifying for such a license in accordance with the rules.

It is noted that, on the whole, the establishment of a RIN and its associated rii for an individual by a jurisdictional domain may be based on, either or a combination of:

1) recognition of the status of an individual

   Basically, these relate to the civil status of an individual in a jurisdictional domain of a geo-political nature, (e.g., such as birth, marriage, death, citizenship, landed immigrant, resident, etc.), and the rights and obligations which are "automatically" conferred relating to the status of an individual.

2) the individual qualifying is based on meeting a set of pre-defined criteria, and passing the associated test.

   On the whole, qualifications of the individual here include:

   a) those of an age nature, i.e. an individual must have attained the age of "n" years to be able to play a particular role, (e.g., get married, authority to buy cigarettes, alcohol, a firearm, vote in local, regional or national elections, etc.;

   b) those of a criteria and/or test nature, in addition to likely having to meet "1)" and "2.a" aspects as well. Examples here include a driver's license, a professional qualification (as an individual qualified and so registered in a recognized "official" profession in a jurisdictional domain), etc.

8.3 Rules governing the assignment of unique identifiers to an individual by Registration Authorities (RAs)

Rule 053:
Any Person acting in the capacity of a Registration Authority (RA) shall, for each of its Registration Schemas (RS) involving the registration of an individual, be identified as observing the rules governing and ensuring the assignment of a unique identifier for that individual as a member of that registration schema.

It is recognized here that the rules governing the eligibility of an individual learner to become a member of a registration schema (RS), administered by its Registration Authority, are for the Registration Authority to determine. This includes determining whether the individual has the qualification to be an eligible candidate in order (to submit a request) to become a member of that Registration Schema including the assignment of a unique identifier (for example is eligible or qualifies to take particular course).

Rule 054:
A Registration Authority shall assign a unique identifier to each of its registered members including, and especially identifying where the member is acting as an individual.

This unique identifier is has the properties and behaviours of an ID code in the coded domain used to support management and maintenance of the Registration Authority Schema[84)]

Rule 055:
Where the Registration Schema (RS) of a Registration Authority allows for the registration of Persons and differentiates among sub-types of Persons, i.e., individuals, organizations and/or public administrations, the Registration Authority shall ensure that:

1) any registration involving an individual is so identified; and,

2) that privacy protection requirements which apply to the resulting personal information are identified and supported.

This is important because where different sub-types of Persons may be members of the same coded domain, resulting from the application of a Registration Schema of a Registration Authority, privacy protection requirements apply only to those members of the coded domain who are individuals. This is because recorded information about a member of a coded domain who is an individual is personal information and thus subject to privacy protection requirements.

Rule 056:
Where a Registration Authority (RA) administers more than one Registration Schema which involves individuals (and their associated personal information), the RA shall not use personal information provided by the individual under one Registration Schema (RS) in another RS of the RA without the explicit consent of the individual concerned.

This rule supports the privacy protection requirements stated in Clause 5.3.4.

8.4 Rules governing individual identity (ies), authentication, recognition, and use

Learning transactions differ in their nature and goals. The rules governing a learning transaction, (a) may allow a Person to use one of several Person identities, (e.g., one of several different credit cards or passports); or, (b) require a Person to have/utilize a pre-specified Person identity (e.g. a Blue Cross card, a national health insurance card, a student identity card, etc.)

[84)] The rules and best practices governing the development, management and interchange of coded domain are the focus of Part 10 “Coded Domains” of the multipart ISO/IEC 15944 multipart standard. Much of the development work for Part 10 has already taken place during the development of the existing parts of ISO/IEC 15944.

Rule 056:
The individual identity, i.e., the persona and the associated identifier, used by an individual in a learning transaction, shall be capable of being prescribed depending on the context and goal of the learning transaction.

Based on the rules in Clause 8.3 and 8.4 above, and drawing on elements in Figure 6 above, Figure 7 below illustrates the range of one-to-one bindings between the personae and identifiers of an individual as individual identities (ii) defined as:

> ***individual identity (ii)***
> ***Person identity*** *of an* ***individual,*** *i.e. an individual identity, consisting of the combination of the* ***persona*** *information and* ***identifier*** *used by an* ***individual*** *in a* ***learning transaction****, i.e. the making of any kind of* ***commitment***

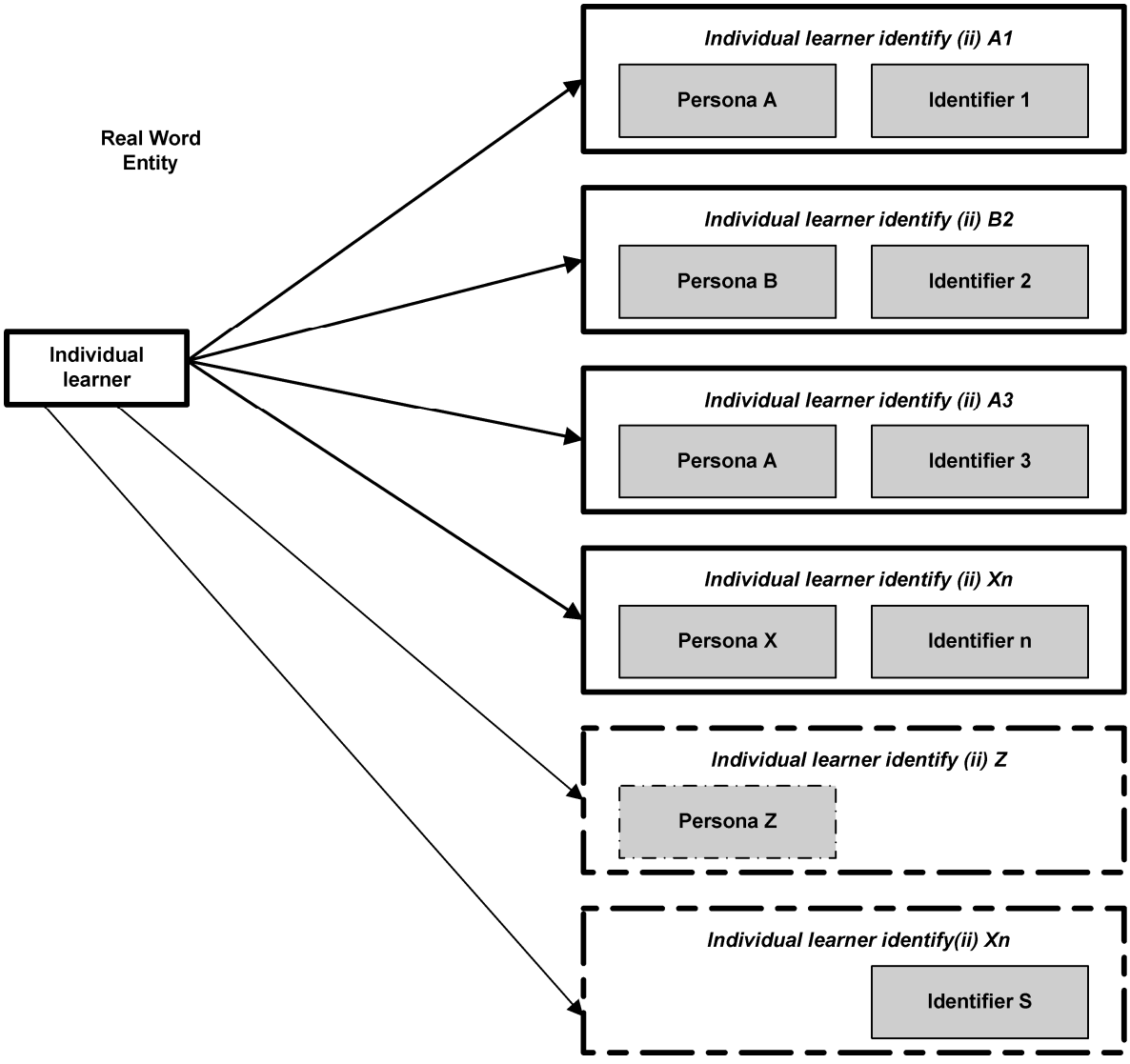

Figure 7 — Illustration of range of links between personae and identifiers of an individual identity (ies) of a learner

Rule 058:

A specific individual identity (ii) established by a registration authority, i.e., organization or public administration, should not be used for any purpose other than that for which it was created, unless with the express and explicit consent of the individual.

Guideline 058G1:
A recognized individual identity (rii) based on a Registration Schema (RS) of Registration Authority (RA) has the added attribute of being re-useable and thus is the preferred approach in support of Open-edi.

A individual identity which is recognized for use in a learning transaction is know as a "recognized individual identity" and is defined based on the existing Part 1 definition of for the concept of "recognized person identity" (rPi)" which has been adapted as follows:

> ***recognized individual identity (rii)***
> *identity of an* ***individual,*** *i.e.,* ***individual identity****, established to the extent necessary for the specific purpose of a learning transaction*

When a Person identity is presented for use in a learning transaction, it has to be "recognized" by the other parties to the learning transaction. Each party to the transaction may have its own rules governing the requirements for establishing a "recognized Person identity (rPi).

Applying the existing ISO/IEC 15944-1 rules governing identification and authentication of Person to an individual learner based on applicable common external constraints, i.e., those stated in Clause 5 above is illustrated in Figure 8 below. It is an adaptation of Figure 12 in Clause 6.2.3 of ISO/IEC 15944-1.

Given the fact that persona Registration Schema (RS), of a Registration Authority (RA),

1) may or may not, include the registration of individuals; and,

2) if the RS, does allow for the registration of individuals as members, then external constraints of a privacy protection requirements nature apply,

it is necessary that one distinguish between a pRS which does not contain individuals as members and those which does, in whole or in part, i.e., as individual persona Registration Schema (ipRS).

Rule 059:
For any persona Registration Schema which includes, in whole or in part, individuals as members, external constraints of a privacy protection nature apply and all its registrants which are individuals shall be managed as members of an individual persona Registration Schema (ipRS) in accordance with applicable privacy protection requirements.

Expanding the definition for the concept of "persona Registration Schema (pRS), an "individual persona Registration Schema (ipRS)" is defined as follows:

> ***individual persona Registration Schema (ipRS)***
> ***persona Registration Schema (pRS)*** *where the* ***persona*** *is, or includes, that of an* ***individual*** *being registered*
>
> NOTE 1 Where an persona Registration Schema includes persona of subtypes of Persons, i.e. individuals, organizations, and/or, public administrations, those which pertain to individuals shall be identified as such because public policy as external constraints apply including those of a privacy protection requirements nature.

NOTE 2 In a individual persona Registration Schema, one shall state whether or not a truncated name, i.e. registered persona, of the individual, is allowed or mandatory, and if so the ipRS shall explicitly state the rules governing the formation of the same.[85)] The selection of an individual identity in a learning transaction between the LET provider and the individual learner as one which is recognized for use between them (as well as any other parties to that learning transaction) is basically established in one of two ways:

1) the individual identity to be recognized (and accepted) for use in a learning transaction is one that is established and mutually agreed to between the buyer and the individual. It is thus a "mutually defined - recognized individual identity (md-rii)".

   Use of such a "md-rii" is found in learning transaction involving internal constraints only. Quite often they are of a one time nature only and not "re-useable". As such, even though the use of a "md-rii" can be modelled in an Open-edi scenario as a scenario component, information bundle, and/or semantic component, it does not have the generally property of re-usability and thus is not a preferred approach in Open-edi.

2) the individual identity to be recognized (and accepted) for use in a learning transaction where the buyer is an individual is one based on that established through a Registration Schema (RS) of a Registration Authority. It is thus a "Registration Schema (based) –recognized individual identity" (RS-rii").

The need be able to support these two basic approaches a recognized identity is supported by two relevant concepts, which are defined as follows:

mutually defined - recognized individual identity (md-rii)
recognized individual identity (rii) *which is mutually defined and agreed to for use between the* ***LET provider*** *and the* ***individual learner,*** *as* ***buyer,*** *in a* ***learning transaction***

NOTE 1 The establishment of a mutually agreed to and recognized individual between a LEET provider and individual learner,, as buyer, does not extinguish the applicable privacy protection rights of that individual.

NOTE 2 A mutually defined recognized individual identity (md-rii) shall be established between the LET provider and the individual learner no later than the end of the negotiation phase.

NOTE 3 Use of a mutually defined recognized individual identity (md-rii) may not be permitted where external constraints apply.

[adapted from ISO/IEC 15944-8, 3.080]

Registration Schema (based) –recognized individual identity (RS-rii)
recognized individual identity (rii) *for use in a* ***learning transaction****, by the buyer as an* ***individual****, which is one based on the use by an* ***individual*** *as a member of a specified* ***Registration Schema (RS)*** *of a particular* ***Registration Authority (RA)***

[adapted from ISO/IEC 15944-8, 3.127]*

[85)] Note the ISO/IEC 7501 multipart standard re "Machine Readable Travel documents" (e.g. passports, already does this. Similarly the ISO/IEC multipart 7812 "Identification cards" standard also does this.

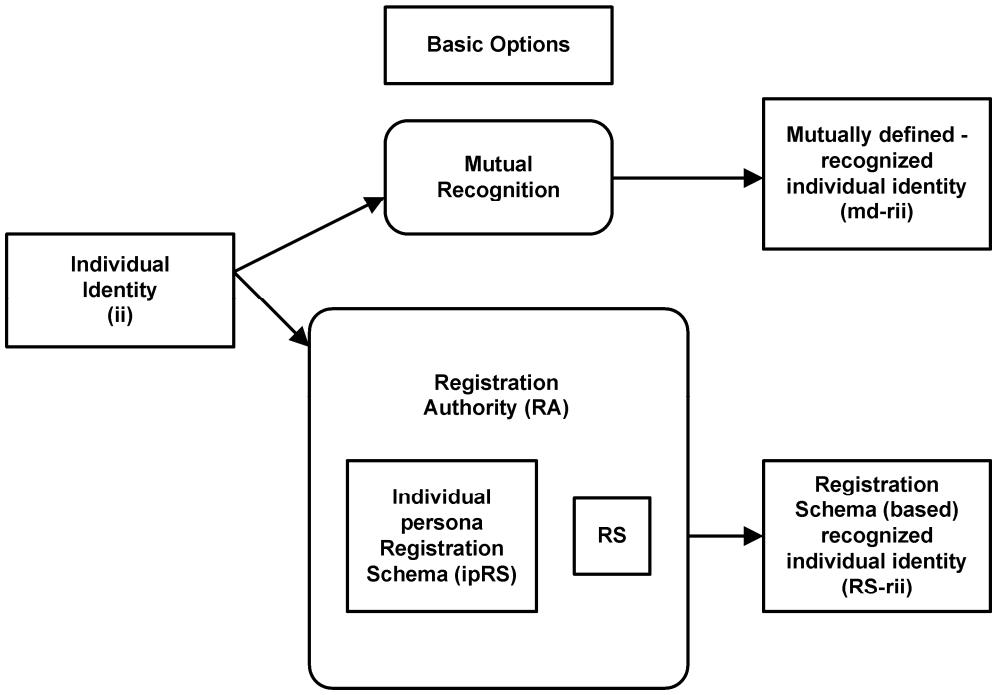

Figure 8 — Illustration of two basic options for establishment of a recognized individual identity (rii)

Rule 060:
A Registration Authority (RA) for individuals shall have explicitly stated rules for transforming an individual identity into a recognized individual identity to meet a stated business requirement.

Rule 061:
The rules governing a learning transaction may either require the use of a specified recognized individual identity (rii) or allow for several of a similar nature.

For example, if payment by credit or debit card is allowed in a learning transaction, several different brands of cards may be allowed, but not necessarily all. It can also happen that for specific learning transactions, an individual may be required to present a "legally" recognized individual identity such as a births certificate, passport, a driver's license, a landed immigrant card, etc.

The establishment or verification of a recognized individual identity will require the capability for authentication, i.e., individual authentication, especially in (electronic) learning transaction. As such individual authentication is defined as:

> ***individual authentication***
> ***provision*** *of the assurance of a* ***recognized individual identity (rii)*** *sufficient for the purpose of the* ***learning transaction***
>
> [adapted from ISO/IEC 15944-8, 3.058]

For individual authentication to be successful, the following actions must have taken place:

1) the individual identity must have been established; and,

2) the individual identity must be recognized, i.e. a recognized individual identity (rii), must exist.

Rule 062:
In a learning transaction, individual authentication is established by either:
1) mutual definition and acceptance: or,

2) referring to predefined individual persona registration schema (ipRS) and process of a particular RA.

8.5 Legally recognized individual identity(ies) (LRIIs)

As was already stated in Part 1 and repeated in this Part 8, a buyer may remain “anonymous” in a learning transaction or use a “pseudonym”. At the other end of the scale the nature of the LET good, service and/or right being provided by the seller (or a regulator as seller) may require a high level of unambiguity as to the identity of the individual. Where this is the case it is most often related to a role qualification the individual needs to have, i.e., as a legally recognized individual identity (LRII) which in turn is issued by a legally (recognized) individual persona Registration Schema (LipRS).

The definitions for these two concepts are as follows:

> ***Legally (recognized) individual persona Registration Schema (LipRS)***
> ***individual persona Registration Schema (ipRS)*** *which has legal status and is so recognized in recognized in a* ***jurisdictional domain*** *as being able to register a* ***recognized individual name (RIN)*** *and unique* ***identifier*** *associated with such a registration*
>
> ***legally recognized individual identity (LRII)***
> ***recognized individual identity (rii)*** *which includes the use of a* ***recognized individual name (RIN)*** *and the associated* ***identifier****, i.e.,* ***ID code****, assigned as part of the* ***personal information*** *for that* ***individual*** *in the* ***individual persona Registration Schema (ipRS)***

Here with respect to a LipRS, it is noted that:

a) at the minimum, they must have the status and recognition in the jurisdiction domain in which they are based;

b) on the whole, the majority of LipRS are the responsibility of a public administration in that jurisdictional domain;

c) where a LipRS is not a public administration its operations and “legally recognized” status is covered through applicable laws and regulations, (e.g., the issuance of credit and debit cards by the financial services sector, the issuance of a diploma, certificate, etc, by a qualified LET institution).

It is recognized that the use of a LRII is directly related to role qualification(s) which apply to a learning transaction. These include those which are:

a) related to the age of the individual concerned to be able to make commitments with respect to certain types of learning transactions such as enrolling in a course, etc.

b) related to the age of an individual and associate role qualification, (e.g., a drivers licence (and most license and certificates) including professional qualifications, (e.g., doctors, plumbers, accountants, lawyers, nurses, etc.).

In addition, a legally recognized individual identity (LRII) may:

a) be of general applicability such as those pertaining the existence and status of an individual (including birth, marriage, or death certificates);

b) have a predefined purpose and use such as a passport, a licence or certificate, a security classification;

c) be used for both individual identity and civil status purposes in a learning transaction;

d) be independent of any particular use even though its use is strictly controlled and regulated by privacy requirements such as any biometric based data used to identify an individual.[86)]

[86)] The standards developed by ISO/IEC JTC1/SC37 *Information technology – biometrics* are relevant here.

9 Person component – individual sub-type

9.1 Introduction

Many aspects of the individual as a sub-type of Person and the resulting link to privacy protection requirements have already been addressed in Clauses 5, 7, and 8 above. This clause sets out additional requirements on the Person component.

9.2 Role qualification of a Person as an individual (learner)

It is very important to ascertain as early as possible whether or not the party to a learning transaction, in the role of a learner, is an individual (or not). The primary reason for this rule is that when the buyer is an "individual", then public policy requirements apply, including privacy protection, consumer protection, individual accessibility, etc. apply {See further Clause 7 above}

Rule 063:
The Clause 8.4 "Rules for the specification of Open-edi roles and role attributes", as stated in ISO/IEC 15944-1:2010 apply, i.e., are mandatory to this Part 1, where the learning transaction involves an individual as a buyer.

Rule 064:
Prior to the start of the actualization phase of a learning transaction, a LET provider shall ascertain whether or not the Person acting as a buyer is doing so in its capacity or status as an individual (rather than as an organization Person or other roles of a Person).

Guideline 064G1:
A LET provider should ascertain at the identification phase in a learning transaction whether or not the Person acting as a buyer is doing so in its capacity or status as an individual and not in one of the other valid capacities of a Person.

It is noted that where LET goods, services and/or rights are offered (sold) by a LET provider to an organization or public administration, privacy protection requirements do (on the whole) not apply.

Rule 065:
Where the learner in a LET transaction is an individual, the LET provider shall:

1) ensure that privacy protection requirements as stated in this standard are applied; and,

2) ascertain whether or not other external constraints apply with respect the individual meeting specified criteria of the applicable jurisdictional domain(s) in qualifying for the role of individual learner with respect to the LET good, service, and/or right which is the goal of the learning transaction.

Rule 066:
When the identification and negation phases of a LET transaction do not result in its actualization and the prospective buyer is an individual, the LET provider (or regulator) shall dispose of all personal information on that individual.

Guideline 066G1:
Where Rule 066 applies, it is best practice that the LET provider or regulator informs the individual that all his/her personal information has been destroyed, [unless the individual requests that his/her personal information be retained, i.e., "left on file"].

{Methodology and tools in support of this requirement are stated in Annex E below}

9.3 Persona and legally recognized names (LRNs) of an individual

As stated in ISO/IEC 15944-1, Clause 6.2.2, a Person may use any persona in a learning transaction as is mutually accepted among all the parties to a learning transaction. This also applies to learning transactions. This internal constraints perspective is qualified where external constraints exist especially those imposed by jurisdictional domains.

However, one result of the application of external constraints is that a Person is not free to choose and negotiate the nature of the Person identify (Pi) to be used in a learning transaction, including the persona forming part of the Pi. Based on the external constraints applicable to the learning transaction, a Person may be required to use a persona which is legally recognized, i.e., has the properties and behaviour of a "legally recognized name (LRN)". This requirement is addressed in Clause 6.6.2.3 "Personae as legally recognized names (LRNs)" ISO/IEC 15944-1. The rules stated in this Clause 6.6.2.3 from a generic Person perspective also apply to ISO/IEC 29187-1

Rule 067:
The rules in Clause 6.6.2.3 "Personae as legally recognized names (LRNs)", as stated in ISO/IEC 15944-5, also apply in this standard.

Rule 068:
Where the buyer in a learning transaction is an individual, the LET provider shall inform the individual as to whether external constraints apply which require the individual to use a legally recognized name (LRN) as its persona as well as the nature Source Authority for such a LRN.

For example, the persona presented by the individual learner for use in a learning transaction must be one which has the status of being legally recognized for use in a jurisdictional domain, (e.g., the persona as stated on a government issued birth certificate, a passport, a driver's licence, health insurance card, etc.).

9.4 Truncation and transliteration of legally recognized names of individuals

In many, if not most jurisdictional domains, there is no legal limit on the length, (number of characters and/or number of discrete character strings) of the persona of an individual, including it being qualified as a LRN. However, standards such as ISO/IEC 7812 for identification cards (including credit/debit cards) and ISO/IEC 7501 for machine-readable travel documents, (e.g., passports), state that the persona has a maximum limited number of characters. The complete persona of a Person may therefore be truncated, i.e., is a "truncated name". Truncated name" is legally recognized and known as a "truncated recognized name (TRN)".

Where a persona of the individual, (e.g., including his/her birth name), as allowed due to external (or internal) constraints of the applicable Registration Schema of the Source Authority, exceeds the maximum number of characters, this persona of the individual needs to be truncated. Therefore, users of this document shall reference and use the ISO 7501 and ISO 7812 standards for the technical rules and details for such truncation.

Rule 69:
The rules governing the truncation of a persona, as stated in ISO 7501 and ISO 7812 apply to this Part of ISO/IEC 29187.

Rule 070:
Where external constraints on a learning transaction require an individual requires as a (potential) learner to use of a legally recognized name (LRN) as the persona for that individual, the LET provider shall specify the types of LRNs permitted to be used by the individual in that learning transaction.

It is a not uncommon occurrence for an individual to move from one jurisdictional domain where the jurisdictional domains have official languages with different writing systems and use of associated distinct character set, (e.g., immigration). In a LET context, a significant number of individual learners do attend schools and universities in other jurisdictional domains. Such international travel in a LET context requires the issuance and use of a passport, which includes the preparation of a Latin-1 character-based persona where the persona of the individual in the jurisdictional domain of that individual uses a non-Latin-1 based character set. this also includes the name of the individual on the application form of the individual learner to a school, university or other LET institution in another jurisdiction domain.

Rule 071:
Where external constraints on a learning transaction require that the persona of the individual be provided in a specified language or character set which is different from the language which the individual uses for his/her persona or birth name, then the transliteration rules of ISO 7501 shall apply[87)]

9.5 Rules governing anonymization of individuals in a learning transaction[88)]

At times, one may not need to distinguish whether the entity which is party to a learning transaction is a "natural person" or "legal person", or an "individual" or "organization", etc. Credit worthiness, ability to pay, secure payment, etc., of a "Person", as a buyer, is often a more important criterion for doing business by the Person in the role of seller based applications, business (including e-commerce, e-government, e-health, e-learning etc.).

In much of consumer trade, a buyer can remain anonymous vis-à-vis a seller by presenting a money token[89)] in which a seller has 100% trust, (e.g., cash). Similarly in (electronic) learning transactions where the value token when presented by the buyer to the seller has 100% trust of the seller, the buyer can also remain anonymous (provided the "E-cash" really has the nature of cash, and does not identify the bearer or holder of the token). Similarly, if a Person (undifferentiated as to organization or individual) with an e-mail address of "diamondsR4ever@google.com" presents an acceptable value token which does not link value token to buyer, the buyer can remain anonymous to the seller.

Thus in electronic learning transactions, unambiguous identification does not necessarily require one to distinguish the nature, i.e., sub-type, of the Person in a learning transaction, i.e., whether the Person is an individual or organization (or an organization Person).[90)]

---

87) These are stated in Annex G to Section IV of ISO/IEC 7501:2006. The source text for which in turn is ICAO document 9303. This Annex G has the following sub-divisions.

A. Transliteration of multinational characters;

B. Transliteration of Cyrillic characters.

Depending on the source text for the persona of individual “A” or “B” apply.These are stated in Annex G to Section IV of ISO/IEC 7501:2006. The source text for which in turn is ICAO document 9303. This Annex G has the following sub-divisions.

88) The text for this sub-Clause is based on Clause D.5.2 of ISO/IEC 15944-1 and other relevant Parts of ISO/IEC 15944 and places these in ISO/IEC 29187-1 privacy protection context.

89) The term “value token” is a generic term used to cover values of a monetary nature such as cash, money orders, bearer bonds, pre-paid value tokens, etc.

90) Privacy concerns of individuals who are worried about who knows what you see and spend online on the Internet with whom, for what, etc., are giving rise to "anonymization services". Disabling "cookies" on one's browser's preferences increasingly prevents prospective buyers from exploring websites of sellers. Such services allow one (1) to browse the Web and go anywhere "cookie free"; (2) to send e-mail through a middle man "remailer"; (3) an anonymous website to allow anyone (individual or organization) to have a homepage without identifying themselves; (4) to support the use of synonyms, etc. {See further, Time, February 8, 1999, p. 62, or visit Internet based services such as <www.anonymize.com>}, www.anonymize.net, www.anonymize.ws>, etc.

Rule 072:
Identification of a Person as LET provider in a learning transaction is not always necessary in (electronic) learning transaction including the LET provider knowing whether or not the individual learner.

For example, an individual can walk into a story purchase a LET course (in physical or electronic form) without being identified to the LET provider.

The Process Component of the Learning transaction Model has five basic sets of activities should be noted, i.e., Planning, Identification, Negotiation, Actualization and Post-Actualization[91)] {see further Clause 10 below} In the Planning set of activities, that is, the first phase in a learning transaction, (prospective) buyers and sellers can and do often remain anonymous to each other. The fundamental characteristic of the Identification Phase is that of establishing one-to-one bindings among the parties (potentially) involved in a learning transaction.

Privacy protection requirements have made "anonymity" an external constraint matter which needs to be supported in this Part 1, i.e., the concept of "individual anonymity" which is defined as follows:

> ***individual anonymity***
> *the state of not knowing the identity or not having any recording of **personal information** on or about an **individual** as a **buyer** by the **seller** or **regulator**, (or any other party) to a **learning transaction)***
>
> *[adapted from ISO/IEC 15944-8, 3.057]*

From a process perspective, "anonymization is defined as follows:

> ***anonymization***
> ***process** whereby the association between **a set of recorded information (SRI)** and an identifiable **individual** is removed, where such an associated existed*
>
> *[adapted from ISO 25237:2008, 3.2]*

Rule 073:
Unless explicitly proscribed, (not allowed) by particular external constraints of the relevant jurisdictional domain applicable to the specified goal of the learning transaction to be entered into, an individual as learner many decide to remain anonymous in that learning transaction, and no personal information on the individual is maintained by the LET provider or regulator.

One common external constraint of a jurisdictional domain is that of stating a role qualification for an individual as a party to a transaction. For example, an individual must be able to provide "proof of age" in the purchase of products which are "age" dependent, (e.g., cigarettes, alcohol, etc.). However, the provision of "proof of age" by an individual (or external constraints of a similar nature) does not necessarily require the capture of any personal information (including any "individual identity") by the seller on the individual as the buyer in that transaction. That is, unless explicitly required by a regulator, the individual identity (and associated personal information) provided by the individual as its "proof of age" is simply "shown" and not recorded. Only the learning transaction identifier generated (on the sales receipt or registration) by the LET provider for an instantiated learning transaction needs to be retained by the parties to the learning transaction. {See further Clause 11.2 below}

---

91) See Clause 6.1.5 and Clause 6.3 "Rules Governing the Process Component" in ISO/IEC 15944-1:2010.

9.6 Rules governing pseudonymization of personal information in a learning transaction[92)]

At times it is desired that an individual can establish a long-term relationship (including a reputation, trust relationship, etc.), with some other Person, without the individual's actual identity being disclosed. For convenience, it may be useful for the individual, or the other party concerned, to establish a unique (new) persona, identifier, token, etc., known as "pseudonym" with the other Person. Pseudonymization is recognized as an important method for privacy protection of personal information. Pseudonymization techniques, mechanisms and services may be used within an organization or public administration, within a jurisdictional domain as a whole or across jurisdictional domains for transborder data flows.

Application areas for pseudonymization include, but are not limited to:

1) secondary use of personal information, (e.g., research);

2) use of pseudonym in publishing; and,

3) use on the internet and other computer networks.

In the context of this standard, a "pseudonym" is defined as follows:

> ***pseudonym***
> *use of a **persona** or other **identifier** by an **individual** which is different from that used by the **individual** with the intention that it be not linkable to that **individual***
>
> *[adapted from ISO TS 25237:2008 (3.4)]*
>
> And in the same context "pseudonymization" is defined as:
>
> ***pseudonymization***
> *particular type of anonymization that removes the associate with an **individual** and adds an associate between a particular set of **characteristics** relating to the **individual** and one more **pseudonym***
>
> *[adapted from ISO TR 25237:2008 (3.39)]*

92) This Clause 9.6 and its rules make extensive use in summary form of ISO TS 25237:2008 (E) titled *"Health Informatics – Pseudonymization"*.

[THIS PAGE IS INTENTIONALLY LEFT BLANK]

10 Process component[93)]

10.1 Introduction

A key aspect of a learning transaction is that it involves a process which as a transaction is viewed ass consisting of a set of five fundamental activities, namely, planning, identification, negotiation, actualization and post-actualization.

In the Clause 10 sub-clauses below, each of these five fundamental activities is defined. Rules from a privacy protection requirements perspective, applicable to each of these fundamental activities are stated. There are however a limited set of rules which apply to all these five fundamental activities. They are as follows:[94)]

Rule 074:
Conceptually, a learning transaction can be considered to be constructed from a set of fundamental activities. They are planning, identification, negotiation, actualization and post-actualization.

Rule 075:
These five fundamental activities may take place in any order.

Rule 076:
A Person may terminate a learning transaction by any agreed method of conclusion

Rule 077:
The five fundamental sets of activities may be completed in a single continuous interactive dialogue or through multiple sets of interactions among the individual learner and LET provider.

10.2 Planning

In the planning phase, both the LET provider and individual learner are engaged in a process to decide what action to take. Basically a LET provider offers a LET product or service or an individual requests a LET product or service. As such, there is no direct binding between a particular identified individual and an identified LET provider.

Privacy protection requirements are not applicable where a prospective individual, as an individual, issues a request for a LET provider, as an organization or public administration, any personal information associated with such a request is considered to be of a “publicly available personal information” nature.

Examples of the use of the planning phase provided by LET provider include the provision of catalogues or “academic calendars” on course offerings, information posted on Websites, etc. Examples of the planning phase for (potential) individual learner’s perspective include requests whether or not a LET provider offers a particular course, programme, etc.

However, as part of the planning phase, a LET provider should make publicly available its privacy policy for which the buyer can be an individual.

---

93) This ISO/IEC 15944-1 standard anticipated the need for privacy protection requirements. See further in this standard Clause 6.3 in Part 1 and its associated Annex F *“(informative) Learning transaction model: process component”* anticipate support for privacy protection requirements.

94) Since a business transaction and a learning transaction are sub-types of a commitment exchanger, this ISO/IEC 29187-1 uses the Clause 6.5 ISO/IEC 19544-1 rules as a basis for Clause 10 in ISO/IEC 29187-1 standard.

10.3 Identification

The identification phase refers to all those actions or events whereby data is interchanged among potential individual learners and LET providers in order to establish a one-to-one linkage, i.e., binding, between a possible seller(s) and a potential buyer(s). The identification phase also includes the exchange of data required to progress from the planning phase to the negotiation phase as is mutually acceptable.

Rule 078:
During the identification phase, the LET provider shall ascertain whether or not the buyer is an individual, and if so, inform the individual of the privacy policy of the LET provider.

A key role of and need for the identification phase, i.e., between the planning phase and the negotiation phase, is to determine whether or not the learning transaction possibly intended to be entered into by the two primary parties involves a Person in the role of an "individual learner" or that of a "non-individual" i.e., a Person in the role of an organization or public administration[95)]

If the buyer in a learning transaction is an "individual", i.e., as an individual learner, then privacy protection requirements apply.

NOTE The text and rules which follow for the Clauses pertaining to negotiation, actualization and post-actualization phases of a learning transaction.

10.4 Negotiation

The negotiation phase covers all those actions and events involving the exchange of SRIs following the identification, i.e., a potential LET provider and individual learner having (1) identified the nature of the goal of the learning transaction as a commitment exchange; and, (2) identified each other at the level of unambiguity, necessary for this mutual agreement.

Rule 079:
Where the LET provider is an individual learner, the end of the negotiation phase shall include the explicit consent and informed of the individual with respect to the provision of its personal information with respect to an identified purpose of the learning transaction. These shall also include, as identified and specified information life cycle management (ILCM) and EDI aspects of such personal information, i.e., as stated in the above Clause 5.3 "Privacy Principles".

Rule 080:
The completion of the negotiation phase is recognized by the LET provider issuing a learning transaction identifier (LTI) to the learning transaction agreed to as an agreed to commitment exchange between the LET provider and the individual learner.

It is understood that after a LET provider may already assigning a (provisional) LTI during the identification phase.

10.5 Actualization

The actualization phase includes as activities or events and associated exchanges of SRIs necessary for the execution and fulfillment of the results of the negotiated goal for the actual learning transaction.

---

95) An example is that of an organization or public administration as a whole undergoing a learning or training process resulting in a certification, (e.g., ISO 9000 or ISO 14000 certified). The goal of the learning transaction is that of the organization achieving/obtaining a specified certificate.

Rule 081:
Where the buyer is an individual learner, the LET provider shall ensure and have in place supporting procedures and mechanisms to support both the generic privacy protection requirements as (1) found in this standard and stated in its rules and guidelines; and, (2) as well as those resulting from the negotiation phase, i.e., as negotiated between the LET provider and the individual learner.

10.6 Post-Actualization

The post-actualization phase includes all the activities and evens and associated exchanges of SRIs that occur between the LET provider and individual learner after the agreed upon LET good, service and/or right, or is deemed to have been delivered.

The most common form of post-actualization activities are those of the nature of warranties, (extended) service contracts, etc. In a LET context, the primary application of the post-actualization phase is that of the LET provider ensuring the ability to be able to provide for many years (decades) SRIs pertaining to the successful completion by an individual learner of a learning transaction, i.e., in the form of “graduation” at a K-12 level, an academic degree, or diploma, a professional certificate, etc. The following set of rules summarizes the privacy protection requirements which apply.

Rule 082:
A LET provider (and its agent(s)) or third party (or any other party to the learning transaction), shall not retain any personal information on the individual learner for any time longer than is consented to by the individual for post-actualization purposes unless external constraints of the applicable jurisdictional domain requires retention of such personal information for a longer period.

Rule 083:
The LET provider shall explicitly state its post-actualization policy with respect to temporal or permanent retention of any or all of the SRIs pertaining to the learning transaction, including those available in summary form as publicly available information.

An example of publicly available information type personal information at the college or university level is that of the names of the individual who received a degree, diploma, certificate of a specified nature in a particular year.

[THIS PAGE IS INTENTIONALLY LEFT BLANK]

11 Data (element) component of a learning transaction

11.1 Introduction[96)]

With respect to a learning transaction, the creation, collection, management, use, interchange of personal information within DMAs of IT system(s) of an organization or public administration takes place at various levels of granularity. The unifying construct in ISO/IEC 29187-1 is that of a set of recorded information (SRI). A SRI can consist of one or more SRIs, (e.g., as both a student record). The more granular components of a student record can also be managed and interchanged as SRIs), (e.g., as data elements, Semantic Components (SCs), or Information Bundles (IBs)) as interchanged among the parties to a learning transaction.

In an Open-edi Framework and Reference Model context, the interchange of personal information as SRIs in a learning transaction is modelled in the form of information bundles (IBs) and semantic components (SCs) with respect to their actual contents.

11.2 Rules governing the role of Learning Transaction Identifier (LTI) in support of privacy protection requirements

Rules governing the need for and role of Learning Transaction Identifiers (LTI) in support of privacy protection requirements in a learning transaction are on the whole very similar to those of a business transaction involving the provision of goods, services, and/or rights by a seller and a buyer where the buyer is an individual.. In the context of this standard and that of a learning transaction that role of the seller is that of a LET provider and the role of the buyer that of an individual learner. Similarly, rules governing the role, establishment and use of a learning transaction identifier (LTI) are based on those which apply to any commitment exchange among autonomous parties resulting in agreement to undertake the resulting transaction.

As such, this Clause 11.2 is based on the generic aspects of the role and requirements for the creation and use of a learning transaction identifier (LTI) which is independent of whether internal or external constraints apply to a generic learning transaction or a regulatory learning transaction (RLT[97)] . {See further Clause 6.6.4.4 Business transaction Identifier (BTI) and its associated rules and definitions in ISO/IEC 15944-1[98)]

Rule 084:
Each instantiated learning transaction involving an individual learner shall have a learning transaction identifier (LTI) assigned by the LET provider and/or a regulator where applicable.

The assignment of the LTI represents the actualization of a learning transaction. When an individual is the learner, privacy protection requirements apply to all personal information pertaining to that learning transaction. This means that the LET provider or regulator when assigning the LTI also binds itself to the privacy protection requirements of the jurisdictional domain of that individual (as well as applicable consumer protection and individual accessibility requirements).

---

96) The text and rules presented here are based on those found in Clause 6.6 “Rules governing the data component” of ISO/IEC 15944-1 as well as Clause 6.6.4 “*Data component”* of ISO/IEC 15944-5. The generic perspectives of Parts 1, 2 and 5 of ISO/IEC 15944 serve as the basis for bringing forward these in summary form in a LET context of privacy protection requirements.

97) The use of the concept “regulatory learning transaction” is used to cover those external constraints of a jurisdictional domain which apply to an individual of a LET transaction and are mandatory in nature. Examples include “mandatory schooling/education” for all individuals in a specified age range”, mandatory education/training” in order for an individual to obtain “recognized” professional qualification.

98) It is advised that users of this standard familiarize themselves with this Clause 6.6.4.4 in Part 5 of ISO/IEC 15944.

Guideline 084G1:
The LET provider (or the regulator) which assigns the LTI to an actualized learning transaction involving an individual should use the LTI as the ID for all the personal information pertaining to that individual learner associated with that learning transaction

Rule 085:
Where an individual as a learner in a learning transaction decides to be anonymous (as permitted by the external constraints of the applicable jurisdictional domain), the learning transaction identifier (LTI) serves as the sole identifier.

Rule 086:
Where the learning transaction is of the nature of a regulatory learning transaction (RLT) and the rules governing the RLT permit an individual to be a buyer, such rules shall explicitly state and define the associated personal information (in conformance with this standard).

The mandatory use of unique LTI in support of a RLT is necessary to be able to support the rules stated in Clause 5 above. This is because of the SRIs pertaining to an instantiated learning transaction (as SRIs) which are of the nature of personal information can be tagged and linked to the applicable LTI and thus managed accordingly from both a privacy protection and information life cycle management (ILCM) requirements perspective.

11.3 Rules governing state of change management of learning transactions in support of privacy protection requirements

A key characteristic of Open-edi is that "parties control and maintain the states of the recorded information" pertaining to the learning transaction of which they are part. {See Clause 5.4, ISO/IEC 14662} As such, it is important to specify whether or not the content of the SRIs, once interchanged among parties to a learning transaction, is allowed to be changed during any phase of the learning transaction. Knowing whether or not state changes are allowed for a specific SRI is important for the management of state description and automated change management of the state machines of the parties involved in an electronic learning transaction.

This general approach to state changes also applies to this Part 1 especially since these are now mandatory requirements in support of privacy protection requirements.

Rule 087:
The rules governing state changes of recorded information as stated in Clause 6.6.4.3 "State Changes" in Part 5 of ISO/IEC 15944 apply and are mandatory to any learning transaction involving an individual learner, i.e., to all resulting personal information pertaining to that learning transaction.

The execution and implementation of these state change rules requires any organization or public administration which collects or creates personal information, to determine whether or not a state change, if any, is allowed once the personal information in relation to a learning transaction has been recorded. This pertains to any type of SRI[99)] including any data elements, semantic components, file record, etc., forming part of the personal information associated with a learning transaction of an individual learner. Annex D below provides a formalized approach to specifying state changes. This Annex D incorporates two coded domains taken from ISO/IEC 15944-5; namely:

Coded Domain ID	Title
ISO/IEC 15944-5:05	Codes for specifying state changes allowed for the values of Information Bundles and Semantic Components
ISO/IEC 15944-5:06	Codes representing store change type for Information Bundles and Semantic Components

[99)] NOTE: here and elsewhere to use of Information Bundles (IBs) and Semantic Component (SC) simply represent two types of SRIs.

11.4 Rules governing records retention of personal information in a learning transaction[100)]

A common requirement of external constraints of a public policy nature is that they mandate records retention (and deletion) requirements. These were further specified in Clause 6.6.4.2 “Records Retention” of ISO/IEC 15944-5. This general approach to records retention also applies to this ISO/IEC 29187-1, especially that there are now mandatory requirements of privacy protection requirements of a learning transaction.

Rule 088:
The rules governing specification of records retention requirements as stated in Clause 8.5.2.8 and 8.5.2.9 in ISO/IEC 15944-1 , and in Clause 6.6.4.2 of ISO/IEC 15944-5 apply and are mandatory to any learning transaction involving an individual as a buyer, i.e., as an individual learner.

Rule 089:
Where the buyer is an individual, the LET provider shall inform the individual learner of all records retention aspects with respect to the sets of recorded information (SRIs) pertaining to the personal information forming part of the learning transaction, and in particular those pertaining to the post-actualization phase.

The execution and implementation of these rules pertaining to record retention of any personal information forming part of recorded information where an individual is a buyer in a learning transaction are stated in Annex D which also incorporates three coded domains taken from ISO/IEC 15944-5; namely:

Coded Domain ID	Title
ISO/IEC 15944-5:02	Codes representing specification of records retention responsibility
ISO/IEC 15944-5:03	Codes representing disposition of recorded information
ISO/IEC 15944-5:04	Codes representing retention triggers

11.5 Rules governing time/date referencing of personal information in a learning transaction

Unambiguous date and time referencing (a.k.a., “temporal referencing”) has always been an important aspect in the recording of the establishment of the commitment exchanges among all parties to a learning transaction. Unambiguity in the specification of temporal referencing has become even more important in the world of learning transactions where “time” has become as important as “date”. This is especially so in online exchanges, (e.g., stock markets, future markets, derivatives, currency hedging, etc.), in auctions, (e.g., eBay) or similar very time sensitive transactions where the level of granularity, i.e., detail or precision, used in temporal referencing is of great importance. For example, in course offering having a limited enrolment where demand exceeds supply, registration of individual learners is “closed once the maximum number of enrolment spaces is filled.

In addition, while based on internal constraints only, the LET provider and individual learner can mutually decide on a common temporal reference schema (including the manner in which an academic year is divided). Where external constraints apply the use of a specific temporal referencing schema may be proscribed. An example here is a specified temporal reference for K-12 registration deadline date.

Rule 090:
The rules governing temporal referencing as stated in Clause 6.6.4.5 “Date/time referencing” as stated in ISO/IEC 15944-5 apply and are mandatory when the individual learner is a buyer in a learning transaction and thus privacy protection requirements apply and shall be supported by the LET provider.

[100)] A primary privacy protection requirement is that personal information pertaining to a learning transaction is that they mandate records retention and deleting requirements. Those of a generic commitment exchange, i.e., transaction nature, have already been specified in Clause 6.6.4.2 “*Records retention requirements*” in ISO/IEC 15944-5.

Rule 091:
Unless otherwise specified and agreed to by the individual learner and LET provider in a learning transaction, the common temporal referencing schema of the jurisdictional domain of the individual applies.

Rule 092:
The temporal referencing schema governing the learning transaction where the buyer is an individual learner shall also be used to ensure deletion of sets of personal information as required by privacy protection requirements.

12 Conformance statement

12.1 Introduction

It is important for an individual learner to be able to know whether or not an organization or public administration, to which that individual is requested to provide personal information in the establishment of a learning transaction, supports and is compliant with applicable privacy protection requirements as stated in this ISO/IEC 29187-1 standard (or subsequent additional more granular privacy protection requirements as stated in Parts 2+ of ISO/IEC 29187). This requirement is not only important within the jurisdictional domain in which the individual user resides but even more so where an individual decides to explore participating in a learning, education and/or training (LET) activity with an organization or public administration located in a another jurisdictional domain.

Similarly, it is important to organizations and/or public administrations to be able to state that they are conformant with ISO/IEC 29187-1 (as well as ISO/IEC 29187-n+ requirements) for several reasons. These include (in no particular order)

1) the assurance to (a prospective) individual learner that the use, management and interchange of any personal information provided by a (prospective) individual learner to a LET provider (of any kind) in the jurisdictional domain of that individual is conformant with:

   a) privacy protection requirements as stated in ISO/IEC 29187-1; and,

   b) any additional privacy protection requirements of that jurisdictional domain.

2) the assurance to a (prospective) individual learner that the LET provider located in a jurisdictional domain other than that of the individual is conformant with the privacy protection requirements as stated in ISO/IEC 29187-1;

3) the fact that the ability of a LET provider being able to state conformance to privacy protection of ISO/IEC 29187-1 (as well as future Parts 2+) is a very positive and quality aspect in the marketing of the LET goods and services being provided on a national, regional, and/or global basis by that LET provider[101)] The two types of conformance statements presented in Clause 12[102)] are at the most primitive level. More detailed conformance statement(s) with associated rules and procedures, including those pertaining to verification are expected to be developed either as Addendum(s) to this 1st edition or as part of the development of a 2nd edition for this Part 1[103)] There are two different categories of conformance statements for this standard; namely:

   a) Category A – ISO/IEC 29187-1 Reference Model; and,

   b) Category B – added ISO/IEC Part n conformance.

The reason for these two categories is to permit users and implementers of ISO/IEC 20187-1 to be conformant to its requirements as well as having additional conformance statements for a particular Part n of ISO/IEC 29187.

[101)] It may well be that as work on this ISO/IEC 29187 multipart standard develops that it will achieve “ISO 9000” type status.

[102)] Clause 12 is modelled on that found in Clause 6 in the 3rd edition for ISO/IEC 14662 (3rd edition) *“Information technology – Open-edi Reference Model*

[103)] NOTE: At present this 1st edition of ISO/IEC 29187-1 supports a self-declaration approach to conformance.

12.2 Conformance to the ISO/IEC 29187-1 Reference Model

Any user/implementer conformance statement of this nature shall state:

a) that it is conformant to the BOV class of standards of ISO/IEC 14662;

b) the list of the basic concepts of the ISO/IEC 29187-1 Framework and Reference Model as stated in ISO/IEC 29187-1 Clause 3 “Definitions”

Any user/implementer conformance statement of this nature shall have text of the following nature:

> “The creation/collection, use, retention, etc., as well as management and interchange of personal information of an individual learner (or any individual) by XYZ [insert name of organization or public administration] with any other party is conformant and consistent with the eleven Privacy Protection principles stated in ISO/IEC 29187-1, its concepts and definitions, rules and related requirements”.

12.3 Conformance to ISO/IEC 29187-2+ parts

Any user/implantation conformance statement of this nature shall have text of the following nature:

> “In addition to conforming to the requirements of ISO/IEC 29187-1, XYZ [insert name of organization or public administration] is conformant and consistent with the added principles, concepts and their definitions, associated rules, and related requirements as stated in ISO/IEC 29187-2+” [insert Part numbers, one or more].

Annex A
(normative)

Consolidated list of terms and definitions with cultural adaptability: ISO English and ISO French language equivalency

A.1 Introduction

This standard maximizes the use of existing standards where and whenever possible including relevant and applicable existing terms and definitions. These are presented in Clause 3 above. This Annex A contains only those new concepts and their definitions introduced in this Part 1, i.e. as ISO English and ISO French language HIEs.

A.2 ISO English and ISO French

This standard recognizes that the use of English and French as natural languages is not uniform or harmonized globally among the various jurisdictional domains which have English and/or French as their official (or de facto) language(s). (Other examples include use of Arabic, German, Portuguese, Russian, Spanish, etc., as official (or de facto) natural languages in various jurisdictional domains).

Consequently, the terms "ISO English" and "ISO French" are used here to indicate the ISO's specialized use of English and French as natural languages in the specific context of international standardization, i.e., as a "special language".

A.3 Cultural adaptability and quality control

ISO/IEC JTC1 has "cultural adaptability" as the third strategic direction which all standards development work should support. The two other existing strategic directions are "portability" and "interoperability". Not all ISO/IEC JTC1 standards are being provided in more than one language, i.e., in addition to "ISO English," in part due to resource constraints.

Terms and definitions are an essential part of a standard. This Annex serves to support the "cultural adaptability" aspects of standards as required by ISO/IEC JTC1. Its purpose is to ensure that if, for whatever reason, an ISO/IEC JTC1 standard is developed in one ISO/IEC "official" language only, at the minimum the terms and definitions are made available in more than one language.[104)] A key benefit of translating terms and definitions is that such work in providing bilingual/multilingual equivalency:

1) should be considered a "quality control check" in that establishing an equivalency in another language ferrets out "hidden" ambiguities in the source language. Often it is only in the translation that ambiguities in the meaning, i.e., semantics, of the term/definition are discovered. Ensuring bilingual/multilingual equivalency of terms/definition should thus be considered akin to a minimum "ISO 9000-like" quality control check; and,

2) is considered a key element in the widespread adoption and use of standards world-wide, especially by users of this standard who include those in various industry sectors, within a legal perspective, policy makers and consumer representatives, other standards developers, IT hardware and service providers, etc.

[104)] Other ISO/IEC member bodies are encouraged to provide bilingual/multilingual equivalencies of terms/definitions for the language(s) in use in their countries.

A.4 Organization of Annex A - Consolidated list of definitions in matrix form

The terms/definitions are organized in matrix form in alphabetical order (English language). The columns in the matrix are as follows:

Col. No.	Use
	IT-Interface – Identification
1	Clause 3 ID (ID definition as per ISO/IEC 29187-1 Clause 3)
2	Source. International standard referenced or that of ISO/IEC 29187-1 itself.
	Human Interface Equivalent (HIE) Components
3	ISO English Language – Term
4	Gender of ISO English Language Term+
5	ISO English Language – Definition
6	ISO French Language - Term
7	Gender of the ISO French language Term+
8	ISO French Language - Definition

The primary reason for organizing the columns in this order is to facilitate the addition of equivalent terms/definitions in other languages as added sets of paired columns, (e.g., Spanish, Japanese, German, Russian, Chinese, etc)[105)]

+ The codes representing gender of terms in natural languages are those found in Clause 9.5 “Gender, and official, de facto, or LRL languages”, and especially its Table 1 – “ISO/IEC 20016-1:01 Codes representing grammatical gender in natural languages”;

1) ISO English, in Column 4, the gender code = “99” since the English language does not have gender in its grammar; and,

2) ISO French, in Column 7, the gender codes are 01 = masculine, 02 = feminine and 03 = neuter

* The use of [French language equivalent required] in Colum (8) means that for these terms and definitions, ISO/IEC 29187-1 itself will be providing the ISO French language equivalent before the FDIS stage.

In summary, the use of “G” in Columns (4) and (7) pertain to the “gender” of the term. The English language has no grammatical gender but the French language does. The codes used here are as follows:

01 = Masculine

02 = Feminine

03 = Neuter

99 = Not Applicable

[105)] See further Part 7 “*eBusiness Vocabulary*” of ISO/IEC 15944 for an implementation of this approach.

A.5 Consolidated list of ISO/IEC 29187-1 Definitions and associated terms

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.001	ISO/IEC 15944-2:2006 (3.1)	address	99	set of **data elements** that specifies a **location** to which a **recorded information** item(s), a business object(s), a material object(s) and/or a Person(s) can be sent or from which it can be received NOTE 1 An address can be specified as either a physical address and/or electronic address. NOTE 2 In the identification, referencing and retrieving of registered business objects, it is necessary to state whether the pertinent **recorded information** is available in both physical and virtual forms. NOTE 3 In the context of Open-edi, a "**recorded information** item" is modelled and registered as an Open-edi scenario (OeS), Information Bundle (IB) or Semantic Component (SC).	adresse	02	ensemble d'**éléments de données** servant à préciser l'**emplacement** où on peut envoyer ou recevoir un élément d'**information enregistrée**, une objet(s) d'affaires d'apprentissage, un objet matériel et/ou une (ou des) Personne(s) NOTE 1 Une adresse peut être spécifiée comme étant physique et/ou électronique. NOTE 2 Dans l'identification, le référencement et l'extraction des objets d'affaires enregistrés, il est nécessaire d'énoncer si l'information enregistrée pertinente est disponible à la fois sous formes physiques et virtuelles. NOTE 3 Dans le contexte de l'EDI-ouvert, un « article d'information enregistrée » est modélisé et enregistré comme scénario d'EDI-ouvert (OeS), Faisceau d'information (IB) ou Composante sémantique (SC).
3.002	ISO/IEC 29187-1 (3.002)	agent (in LET privacy protection)	99	**Person** acting for another **Person** in a clearly specified capacity in the context of a **learning transaction** NOTE 1 Excluded here are agents as "automatons" (or robots, bobots, etc.). In ISO/IEC 14662, "automatons" are recognized and provided for but as part of the Functional Service View (FSV) where they are defined as an "Information Processing Domain (IPD)". NOTE 2 Adapted from ISO/IEC 15944-1.	mandataire (dans la protection de la vie privée concernant l'AÈF)	01	**Personne** agissant au nom d'une autre **Personne** à titre précis dans le contexte d'une **transaction d'apprentissage** NOTE 1 Sont exclus les mandataires tels que les « automates » (ou les robots, bobots, etc.). Dans la norme ISO/CEI 14662, les « automates » sont pris en compte et prévus, mais à titre de Vue de services fonctionnels (FSV), où ils sont définis comme « domaine de traitement de l'information (IPD)». NOTE 2 Adapté de l'ISO/CEI 15944-1.
3.003	ISO/IEC 15944-8 (3.003)	anonymization	99	**process** whereby the association between a **set of recorded information (SRI)** and an identifiable **individual** is removed where such an association may have existed NOTE Adapted from ISO 25237.	anonymisation	02	**processus** ou est supprimée la corrélation entre un **ensemble d'informations enregistrées (EIE)** et un **individu** identifiable, alors même qu'une telle corrélation a pu préalablement exister NOTE Adapté de l'ISO 25237.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.004	ISO/IEC 11179-3:2003 (3.1.3)	attribute	99	**characteristic** of an **object** or **entity**	attribut	01	**caractéristique** d'un **objet** ou d'une **entité**
3.005	ISO/IEC 10181-2:1996 (3.3)	authentication	99	provision of assurance of the claimed identity of an **entity**	authentification	02	attestation de l'identité revendiquée par une **entité**
3.006	ISO/IEC TR 13335-1:1996 (3.3)	authenticity	99	**property** that ensures that the identity of a subject or resource is the one claimed NOTE Authenticity applies to entities such as users, processes, systems and information.	authenticité	02	**propriété** assurant que l'identité d'un sujet ou d'une ressource est celle qui est prétendue NOTE L'authenticité s'applique à des entités telles que des utilisateurs, des processus, des systèmes et des informations.
3.007	ISO/IEC 14662: 2010 (3.2)	business	99	series of **processes**, each having a clearly understood purpose, involving more than one **Person**, realized through the exchange of **recorded information** and directed towards some mutually agreed upon goal, extending over a period of time	affaires	02	série de **processus**, ayant chacun une finalité clairement définie, impliquant plus d'une **Personne**, réalisés par échange d'**information enregistrée** et tendant à l'accomplissement d'un objectif accepté par accord mutuel pour une certaine période de temps
3.008	ISO/IEC 15944-1:2011 (3.8)	buyer	99	**Person** who aims to get possession of a good, service and/or right through providing an acceptable equivalent value, usually in money, to the **Person** providing such a good, service and/or right	acheteur	01	**Personne** désirant acquérir un bien, service et/ou droit en fournissant une valeur équivalente acceptable, généralement de l'argent, à la **Personne** qui offre ce bien, service et/ou droit
3.009	ISO 1087-1:2000 (3.2.4)	characteristic	99	abstraction of a **property** of an **object** or of a set of **objects** NOTE Characteristics are used for describing concepts.	caractère	01	**propriété** abstraite d'un **objet** ou d'un ensemble d'**objets** NOTE Les caractères servent à décrire les concepts.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.010	ISO/IEC 2382-4:1999 (04.01.02)	character set	99	finite set of different **characters** that is complete for a given purpose EXAMPLE The international reference version of the character set of ISO 10646.	jeu de caractères	01	ensemble fini de différents **caractères** considéré comme complet à des fins déterminé(e)s EXEMPLE La version internationale de référence du jeu de caractères de l'ISO 10646.
3.011	ISO/IEC 29187-1 (3.011)	classification system (in LET privacy protection)	99	systematic **identification** and arrangement of learning activities and/or **scenario components** into categories according to logically structured conventions, methods and procedural **rules** as specified in a classification schema NOTE 1 The classification code or number often serves as a semantic identifier (SI) for which one or more human interface equivalents exist. NOTE 2 The rules of a classification schema governing the operation of a classification system at times lead to the use of ID codes which have an intelligence built into them, (e.g., in the structure of the ID, the manner in which it can be parsed, etc. Here the use of block-numeric numbering schemas is an often used convention. NOTE 3 Adapted from ISO/IEC 15944-5.	système de classification (dans la protection de la vie privée concernant l'AĖF)	01	**identification** et arrangement systématiques des activités **d'apprentissage** et/ou des **composantes de scénario** en catégories selon des conventions, des méthodes et des **règles** de procédure structurées logiquement, tel que spécifié dans un schéma de classification NOTE 1 Le code ou numéro de classification sert souvent d'identificateur sémantique (SI) pour lequel existent un ou plusieurs équivalents d'interface humaine. NOTE 2 Les règles d'un schéma de classification régissant l'exploitation d'un système de classification mènent parfois à l'utilisation de codes ID à intelligence intégrée (par ex. dans la structure de ns ces cas. NOTE 3 Adapté de l'ISO/CEI 15944-5.
3.012	ISO 639-2:1998 (3.1)	code	99	**data** representation in different forms according to a pre-established set of **rules** NOTE In this standard, the, the "pre-established set of rules" are determined and enacted by a Source Authority and must be explicitly stated.	code	01	représentation de **données** sous différentes formes, écrites selon un jeu de **règles** préétablies NOTE Dans cette norme,, "l'ensemble de règles préétablies" est déterminé et mis en vigueur par une Autorité de source et doit être énoncé explicitement.
3.013	ISO/IEC 15944-5:2008 (3:19)	code (in coded domain)	99	**identifier**, i.e., an **ID code**, assigned to an **entity** as member of a **coded domain** according to the pre-established set of **rules** governing that **coded domain**	code (dans un domaine codé)	01	**identificateur**, c.-à.-d. **code ID**, attribué à une **entité** en tant que membre d'un **domaine codé** conformément à l'ensemble de **règles** régissant ce **domaine codé**

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.014	ISO/IEC 15944-2:2006 (3.13)	coded domain	99	domain for which (1) the boundaries are defined and explicitly stated as a **rulebase** of a **coded domain Source Authority**; and, (2) each **entity** which qualifies as a member of that domain is identified through the assignment of a unique **ID code** in accordance with the applicable **Registration Schema** of that **Source Authority** NOTE 1 The rules governing the assignment of an ID code to members of a coded domain reside with its Source Authority and form part of the Coded Domain Registration Schema of the Source Authority. NOTE 2 Source Authorities which are jurisdictional domains are the primary source of coded domains. NOTE 3 A coded domain is a data set for which the contents of the data element values are predetermined and defined according to the rulebase of its Source Authority and as such have predefined semantics. NOTE 4 Associated with a code in a coded domain can be: (a) one and/or more equivalent codes; (b) one and/or more equivalent representations especially those in the form of Human Interface Equivalent (HIE) (linguistic) expressions. NOTE 5 In a coded domain the rules for assignment and structuring of the ID codes must be specified. NOTE 6 Where an entity as member of a coded domain is allowed to have, i.e., assigned, more than one ID code, i.e., as equivalent ID codes (possibly including names), one of these must be specified as the pivot ID code NOTE 7 A coded domain in turn can consist of two or more coded domains, i.e., through the application of the inheritance principle of object classes. NOTE 8 A coded domain may contain an ID code which pertains to predefined conditions other than qualification of membership of entities in the coded domain. Further, the rules governing a coded domain may or may not provide for user extensions.	domaine codé	01	domaine pour lequel (1) les limites sont définies et explicitement énoncées comme **base de règles** de l'**Autorité de source** d'un **domaine codé** ; et, (2) chaque **entité** se qualifiant comme membre de ce domaine est identifiée grâce à l'attribution d'un **code ID** unique conformément au **Schéma d'enregistrement** applicable de cette **Autorité de source** NOTE 1 Les règles régissant l'attribution d'un code aux membres d'un domaine codé résident dans son Autorité de source et font partie du Schéma d'enregistrement du domaine codé de l'Autorité de source. NOTE 2 Les Autorités de source qui sont des domaines juridictionnels sont la source primaire des domaines codés. NOTE 3 Un domaine codé est un ensemble de données pour lequel le contenu des valeurs des éléments de données est prédéterminé et défini conformément à la base de règles de son Autorité de source et, à ce titre, à une sémantique prédéfinie. NOTE 4 Peuvent être associés à un code dans un domaine codé : un ou plusieurs codes équivalents : (a) - un et/ou plusieurs codes équivalentes; et/ou, (b) une ou plusieurs représentations équivalentes, surtout celles qui sont sous forme d'expressions d'Équivalents d'interface humaine (EIH) (linguistique). NOTE 5 Dans un domaine codé, les règles d'attribution et de structuration des codes d'identité doivent être spécifiées. NOTE 6 Lorsqu'on permet à une identité à titre de membre d'un domaine codé d'avoir, c.-à-d. de se voir attribué, plus d'un code d'identité, c.-à-d. des codes d'identité équivalents (pouvant inclure des noms), l'un de ces codes doit être spécifié à titre de code d'identité pivot. NOTE 7 Un domaine codé peut à son tour se composer de plusieurs domaines codés grâce à l'application du principe d'héritage des classes d'objet. NOTE 8 Un domaine codé peut contenir un code d'identité relatif à des conditions prédéfinies autres que la qualification d'appartenance des entités du domaine codé. De plus, les règles régissant un domaine codé peuvent ou non contenir des extensions utilisateur.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				EXAMPLE Common examples include: (1) the use of ID Code "0" (or "00", etc.) for “Others, (2) the use of ID Code "9" (or "99", etc.) for “Not Applicable”; (3) the use of “8” (or “98”) for “Not Known”; and/or, if required, (4) the pre-reservation of a series of ID codes for use of “user extensions”. NOTE 9 In object methodology, entities which are members of a coded domain are referred to as instances of a class. EXAMPLE In UML modelling notation, an ID code is viewed as an instance of an object class.			EXEMPLE Exemples courants : (1) l’utilisation du code d’identité « 0 » (ou « 00 », etc.) pour « Autres », (2) l’utilisation du code d’identité « 9 » (ou « 99 », etc.) pour « Sans objet »; (3) l’utilisation du code d’identité « 8 » (ou « 98 ») pour « Inconnu »; et/ou, si nécessaire, (4) la pré-réservation d’une série de codes d’identité pour l’utilisation d’extensions utilisateur ». NOTE 9 Dans la méthodologie objet, les entités membres d’un domaine codé s’appellent « instances d’une classe ». EXEMPLE Dans la notation modélisée UML, un code d’identité est considéré comme une instance de classe d’objet.
3.015	ISO/IEC 15944-5:2008 (3.21)	coded Domain Registration Schema (cdRS)	99	formal **definition** of both (1) the **data** fields contained in the **identification** and specification of an **entity** forming part of the members a **coded domain** including the allowable contents of those fields; and, (2) the **rules** for the assignment of **identifiers**	Schéma d’enregis-trementent du domaine codé (cdRS)	01	**définition** formelle à la fois des (1) champs de **données** contenus dans l’**identification** et la spécification d’une **entité** faisant partie des membres d’un **domaine codé** (y compris les contenus permis de ces champs) ; et (2) **règles** d’attribution des **identificateurs**
3.016	ISO/IEC 15944-2:2006 (3.14)	coded domain Source Authority (cdSA)	99	**Person**, usually an **organization**, as a **Source Authority** which sets the **rules** governing a **coded domain** NOTE 1 Source Authority is a role of a Person and for widely used coded domains the coded domain Source Authority is often a jurisdictional domain. NOTE 2 Specific sectors, (e.g., banking, transport, geomatics, agriculture, etc.), may have particular coded domain Source Authority(Authority (ies) whose coded domains are used in many other sectors. NOTE 3 A coded domain Source Authority usually also functions as a Registration Authority but can use an agent, i.e., another Person, to execute the registration function on its behalf.	Autorité de source du domaine codé (cdSA)	02	**Personne**, habituellement une **organisation**, qui établit les **règles** régissant un **domaine codé** en tant qu’**Autorité de source** NOTE 1 L’Autorité de source est un rôle d’une Personne et, pour les domaines codés largement utilisés, l’Autorité de source du domaine codé est souvent un domaine juridictionnel. NOTE 2 Des secteurs spécifiques (par ex. le domaine bancaire, les transports, la géomètre, l’agriculture, etc.) peuvent avoir une (des) Autorité(s) de source du domaine codé dont les domaines codés sont utilisés dans d’autres secteurs. NOTE 3 Une Autorité de source du domaine codé fonctionne aussi habituellement comme Autorité d’enregistrement, mais peut utiliser un agent, c.-à.-d. une autre Personne, pour exécuter la fonction d’enregistrement à sa place.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.017	ISO/IEC 15944-4:2007 (3.12)	collaboration space	99	**business** activity space where an economic exchange of valued resources is viewed independently and not from the perspective of any **business** partner NOTE In collaboration space, an individual partner's view of economic phenomena is de-emphasized. Thus, the common use business and accounting terms like purchase, sale, cash receipt, cash disbursement, raw materials, and finished goods is not allowed because they view resource flows from a participant's perspective.	espace de collaborative	01	espace d'activité d'**affaires** dans lequel un échange économique de ressources valorisées est considéré indépendamment et non du point de vue de tout partenaire d'**affaires** NOTE Dans l'espace de collaboration, la perspective qu'un partenaire individuel a d'un phénomène économique est désaccentuée. Ainsi, les termes d'affaires et de comptabilité communément utilisés tels que achat, vente, reçu de caisse, décaissement, matières premières, produits finis, etc. ne sont pas autorisés à être utilisés car ils considèrent les flux de ressources du point de vue d'un participant.
3.018	ISO/IEC 14662:2010 (3.5)	commitment	99	making or accepting of a right, obligation, liability or responsibility by a **Person** that is capable of enforcement in the **jurisdictional domain** in which the **commitment** is made	engagement	01	création ou acceptation d'un droit, d'une obligation, d'une dette ou d'une responsabilité par une **Personne** qui est apte à appliquer le **domaine juridictionnel** conformément à laquelle l'**engagement** est pris
3.019	ISO/IEC 29187-1 (3.019)	composite identifier (in LET privacy protection)	99	**identifier** (in a **learning transaction**) functioning as a single unique **identifier** consisting of one or more other **identifiers**, and/or one or more other **data elements**, whose interworking are **rule**-based NOTE 1 Identifiers (in learning transactions) are for the most part composite identifiers. NOTE 2 The rules governing the structure and working of a composite identifier should be specified. NOTE 3 Most widely used composite identifiers consist of the combinations of: (1) the ID of the overall identification/numbering schema, (e.g., ISO/IEC 6532, ISO/IEC 7812, ISO/IEC 7506, UPC/EAN, ITU-T E.164, etc.), which is often assumed; (2) the ID of the issuing organization (often based on a block numeric numbering schema); and, (3) the ID of the entities forming part of members of the coded domain of each issuing organization. NOTE 4 Adapted from ISO/IEC 15944-8.	identificateur composite (dans la protection de la vie privée concernant l'AÉF)	01	**identificateur** (dans une **transaction d'apprentissage** fonctionnant comme élément **identificateur** simple et unique comprenant un ou plusieurs autres **identificateurs** et/ou un ou plusieurs **éléments de données**, dont les interconnexions sont basées sur des **règles** NOTE 1 Les identificateurs (dans les transactions d'apprentissage sont pour la plupart des identificateurs composites. NOTES 2 Les règles régissant la structure et le fonctionnement d'un identificateur composite doivent être spécifiées. NOTE 3 Les identificateurs composites les plus communément utilisés se composent de combinaisons: (1) de l'identité du schéma d'identification/numérotation global, (par ex. ISO/IEC 6532, ISO/CIE 7812, ISO/CIE 7506, UPC/EAN, ITU-T E.164, etc.), qui est souvent assumé ; (2) de l'identité de l'organisation émettrice (souvent basé sur un schéma de numérotation numérique par blocs); et, (3) l'identité des entités faisant partie de membres du domaine codé de chaque organisation émettrice. NOTE 4 Adapté de l'ISO/CEI 15944-8.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.020	ISO/IEC 15944-2:2006 (3.18)	computational integrity	99	expression of a **standard** in a form that ensures precise description of behaviour and semantics in a manner that allows for automated processing to occur, and the managed evolution of such **standards** in a way that enables dynamic introduction by the next generation of information systems NOTE Open-edi standards have been designed to be able to support computational integrity requirements especially from a registration and re-use of business objects perspectives.	intégrité informatique	02	expression d'une **norme** sous une forme qui assure la description précise du comportement et de la sémantique d'une façon qui permet un traitement automatique, ainsi que l'évolution gérée de ces **normes** d'une manière qui permet une introduction dynamique par la génération suivante de systèmes informatiques NOTE Les normes de l'EDI-ouvert ont été conçues pour pouvoir appuyer les exigences en matière d'intégrité computationnelle, particulièrement dans des perspectives d'enregistrement et de réutilisation des objets d'affaires.
3.021	ISO/IEC 29187-1 (3.021)	constraint (in LET privacy protection)	99	**rule**, explicitly stated, that prescribes, limits, governs or specifies any aspect of a **learning transaction** NOTE 1 Constraints are specified as rules forming part of components of Open-edi scenarios, i.e., as scenario attributes, roles, and/or information bundles. NOTE 2 For constraints to be registered for implementation in Open-edi, they must have unique and unambiguous identifiers. NOTE 3 A constraint may be agreed to among parties (condition of contract) and is therefore considered an "internal constraint". Or a constraint may be imposed on parties, (e.g., laws, regulations, etc.), and is therefore considered an "external constraint". NOTE 4 Adapted from ISO/IEC15944-1.	contrainte (dans la protection de la vie privée concernant l'AĖF)	02	**règle**, énoncée explicitement, qui prescrit, limite, régit ou spécifie tout aspect d'une **transaction d'apprentissage** NOTE 1 Les contraintes sont spécifiées comme des règles faisant partie de composantes de scénarios d'EDI-ouvert, c.-à-d. d'attributs de scénarios, de rôles, et/ou de faisceaux d'information. NOTE 2 Les contraintes doivent avoir des identificateurs uniques et non-ambigus afin d'être enregistrées pour application dans l'EDI-ouvert. NOTE 3 Une contrainte peut faire l'objet d'un accord entre des parties (clause du contrat), et est par conséquent considérée comme « contrainte interne ». Ou une contrainte peut être imposée à des parties, (par ex. des lois, des règlements, etc.), et est par conséquent considérée comme une « contrainte externe ». NOTE 4 Adapté de l'ISO/IEC 15944-1.
3.022	ISO/IEC 15944-1:2011 (3.12)	consumer	99	**buyer** who is an **individual** to whom **consumer protection** requirements are applied as a set of **external constraints** on a **business** transaction NOTE 1 Consumer protection is a set of explicitly defined rights and obligations applicable as external constraints on a learning transaction. NOTE 2 The assumption is that a consumer protection applies only where a buyer in a learning transaction is an individual. If this is not the case in a particular jurisdiction, such external constraints should be specified as part of scenario components as applicable.	consommateur	01	**acheteur**, en tant qu'**individu**, auquel s'appliquent des exigences de **protection des consommateurs** comme ensemble de **contraintes externes** sur une transaction d'**affaires** NOTE 1 La protection des consommateurs est un ensemble de droits et d'obligations définis explicitement et qui s'appliquent à titre de contraintes externes à une transaction d'apprentissage. NOTE 2 Le postulat est que la protection des consommateurs s'applique uniquement lorsqu'un acheteur dans une transaction d'apprentissage est un individu. Si ce n'est pas le cas dans une juridiction particulière, il faut spécifier ces contraintes externes comme faisant partie de composantes de scénarios selon le cas.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 3 It is recognized that external constraints on a buyer of the nature of consumer protection may be peculiar to a specified jurisdictional domain.			NOTE 3 On reconnaît que les contraintes externes de protection des consommateurs exercées sur un acheteur peuvent relever d'une juridiction particulière.
3.023	ISO/IEC 15944-5:2008 (3.33)	consumer protection	99	set of **external constraints** of a **jurisdictional domain** as rights of a **consumer** and thus as obligations (and possible liabilities) of a **vendor** in a **business transaction** which apply to the good, service and/or right forming the **object** of the **business transaction** (including associated information management and interchange requirements including applicable (sets of) **recorded information**) NOTE 1 Jurisdictional domains may restrict the application of their consumer protection requirements as applicable only to individuals engaged in a business transaction of a commercial activity undertaken for personal, family or household purposes, i.e., they do not apply to natural persons in their role as "organization" or "organization **Person**". NOTE 2 Jurisdictional domains may have particular consumer protection requirements which apply specifically to individuals who are considered to be a "child" or a “minor”, (e.g., those individuals who have not reached their thirteenth (13) birthday). NOTE 3 Some jurisdictional domains may have consumer protection requirements which are particular to the nature of the good, service and/or right being part of the goal of a business transaction.	protection du consommateur	02	ensemble de **contraintes externes** d’un **domaine juridictionnel** comme droits d’un **consommateur** et ainsi comme obligations (et responsabilités éventuelles) d’un **fournisseur** dans une **transaction d’affaires** qui s’applique au bien, au service et/ou droit faisant l’**objet** de la **transaction d’affaires** (y compris les exigences en matière de gestion et l’échange de l’information qui s’y rattachent, dont l’(ou l’ensemble des) **information enregistrée** applicable NOTE 1 Des domaines juridictionnels peuvent restreindre l’application de leurs exigences en matière de protection du consommateur comme applicables uniquement aux individus participant à une transaction d’apprentissage de nature commerciale entreprise à des fins personnelles, familiales ou domestiques, c.-à.-d. qu’ils ne s’appliquent pas aux personnes physiques dans leur rôle d’ « organisation » ou de « Personne d’organisation ». NOTE 2 Des domaines juridictionnels peuvent avoir des exigences particulières en matière de protection du consommateur qui s’appliquent spécifiquement à un individu considérés comme un « enfant » ou un « mineur » (par ex. les individus n’ayant pas encore atteint leur treizième anniversaire de naissance). NOTE 3 Certains domaines juridictionnels peuvent avoir des exigences en matière de protection du consommateur propres à la nature du bien, du service, et/ou du droit faisant l’objet d’une transaction d’affaires.
3.024	ISO/IEC 15944-5:2008 (3.34)	controlled vocabulary (CV)	99	**vocabulary** for which the entries, i.e., **definition/term** pairs, are controlled by a **Source Authority** based on a **rulebase** and **process** for addition/deletion of entries NOTE 1 In a controlled vocabulary, there is a one-to-one relationship of definition and term. EXAMPLE The contents of "Clause 3 Definitions" in ISO/IEC standards are examples of controlled vocabularies with the entities being identified and referenced through their ID code, i.e., via their clause numbers.	vocabulaire contrôlé (CV)	01	**vocabulaire** dont les entrées, c.-à.-d. les paires de **termes et définitions**, sont contrôlées par une **Autorité de sourc**e fondée sur une **base de règles** et un **processus** pour ajouter et supprimer des entrées NOTE 1 Dans un vocabulaire contrôlé, une correspondance biunivoque existe entre le terme et sa définition. EXEMPLE Le contenu des « Définitions de la Clause 3 » des normes ISO/CEI sont des exemples de vocabulaires contrôlés dont les entités sont identifiées et référencées grâce à leur code ID, c.-à.-d. leur numéro de clause.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 2 In a multilingual controlled vocabulary, the definition/term pairs in the languages used are deemed to be equivalent, i.e., with respect to their semantics. NOTE 3 The rule base governing a controlled vocabulary may include a predefined concept system.			NOTE 2 Dans un vocabulaire contrôlé multilingue, les paires de termes/définitions des langues utilisées sont jugées sémantiquement équivalentes. NOTE 3 La base de règles régissant un vocabulaire contrôlé peut inclure un système de concepts prédéfini.
3.025	ISO/IEC 29187-1 (3.025)	data (in a learning transaction)	99	representations of **recorded information** that are being prepared or have been prepared in a form suitable for use in a computer system NOTE Adapted from ISO/IEC 15944-1.	donnée (dans une transaction d'apprentissage)	02	représentations d'**informations enregistrées** qui sont préparées ou l'ont été de façon à pouvoir être traitée par un ordinateur NOTE Adapté de l'ISO/ICEI 15944-1.
3.026	ISO/IEC 11179-1:2004 (3.3.8)	data element	99	unit of **data** for which the **definition**, **identification**, representation and permissible values are specified by means of a set of **attributes**	élément de données	01	unité de **données** dont la **définition**, l'**identification**, la représentation et les valeurs autorisées sont spécifiées au moyen d'un ensemble d'**attributs**
3.027	ISO/IEC 2382-4:1999 (04.07.01)	data element (in organization of data)	99	unit of **data** that is considered in context to be indivisible EXAMPLE The data element "age of a **Person**" with values consisting of all combinations of 3 decimal digits. NOTE Differs from the entry 17.06.02 in ISO/IEC 2382-17.	élément de données (en organisation de données)	01	**donnée** considéré comme indivisible dans un certain contexte EXEMPLE L'élément de données «âge d'une personne» avec des valeurs comprenant toutes les combinaisons de trois chiffres décimaux. NOTE Cette notion est différente de celle de l'article 17.06.02 dans la norme ISO/CEI 2382-17.
3.028	ISO 19115:2003 (4.2)	dataset	99	identifiable collection of **data** NOTE A dataset may be a smaller grouping of data which, though limited by some constraint such as spatial extent or feature type, is located physically within a larger dataset. Theoretically, a dataset may be as small as a single feature or feature attribute contained within a larger dataset. A hardcopy map or chart may be considered a dataset.	ensemble de données	01	collecte de **données** identifiables NOTE Un ensemble de données peut être un groupement plus petit données qui, bien que limité par certaines contraintes telles que l'étendue spatiale ou le type de caractéristique, est situé physiquement dans un ensemble de données plus étendu. En théorie, un ensemble de données peut être aussi petit qu'une caractéristique unique ou un attribut de caractéristique contenu dans un ensemble de données plus étendu.
3.029	ISO 19115:2003 (4.3)	dataset series	99	collection of **datasets** sharing the same product specification	série de données	02	collecte d'**ensemble de données** partageant la même spécification de produit
3.030	ISO/IEC 29187-1 (3.030)	data synchronization (in learning transaction)	99	**process** of continuous harmonization of a **set(s)** of **recorded information** among all the parties to a **learning transaction** to ensure that the current state of such a **set(s)** of **recorded information** is the same in the **IT systems** of all the participating parties NOTE 1 Adapted from ISO/IEC 15944-8.	synchronisation des données (dans une transaction d'apprentissage)	02	**processus** d'harmonisation continue d'éléments d'**information enregistrée** entre les partenaires d'une **transaction d'apprentissage**, dans le but de s'assurer que ces éléments d'**information enregistrée** sont semblables dans les systèmes d'**information** de toutes les parties participantes. NOTE 1 Adapté de L'ISO/CEI 15944-8.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.031	ISO/IEC 14662:2010 (3.6)	Decision Making Application (DMA)	99	**model** of that part of an **Open-edi system** that makes decisions corresponding to the **role**(s) that the **Open-edi Party** plays as well as the originating, receiving and managing **data** values contained in the instantiated **Information Bundles** which is not required to be visible to the other **Open-edi Party(ies)**	Application à pouvoir de décision (DMA)	02	**modèle** de la partie d'un système d'**EDI-ouvert** qui prend les décisions correspondant au **rôle** ou aux **rôles** que joue le **partenaire** d'**EDI-ouvert**; elle est aussi source, récepteur et gestionnaire des valeurs des **données** contenues dans les instances de **faisceaux d'informations**; elle n'a pas à être rendue visible au(x) autre(s) **partenaire(s) d'EDI-ouvert**
3.032	ISO/IEC 15944-5:2008 (3.42)	de facto language	99	**natural language** used in a **jurisdictional domain** which has the properties and behaviours of an **official language** in that **jurisdictional domain** without having formally been declared as such by that **jurisdictional domain** NOTE 1 A de facto language of a jurisdictional domain is often established through long term use and custom. NOTE 2 Unless explicitly stated otherwise and for the purposes of modelling a learning transaction through scenario(s), scenario attributes and/or scenario components, a de facto language of a jurisdictional domain is assumed to have the same properties and behaviours of an official language.	langue de facto	02	**langage naturel** utilise dans un **domaine juridictionnel** qui a les propriétés et comportement d'une **langue officielle** dans ce **domaine juridictionnel** sans avoir été formellement déclaré comme telle par ce **domaine juridictionnel** NOTE 1 Une langue de facto d'un domaine juridictionnel est souvent établie à travers un usage et des coutumes à long terme. NOTE 2 Sauf énoncé explicite contraire et aux fins de modélisation d'une transaction d'apprentissage à travers un (ou des) scénario(s), attribut(s) de scénario et/ou composantes de scénario, une langue de facto d'un domaine juridictionnel est suppose avoir les mêmes propriétés et comportements qu'une langue officielle.
3.033	ISO 1087-1:2000 (3.3.1)	definition	99	representation of a concept by a descriptive statement which serves to differentiate it from related concepts	définition	02	représentation d'un concept au moyen d'un énoncé descriptif qui sert à la différencier d'autres concepts
3.034	ISO 1087-1:2000 (3.4.1)	designation	99	representation of a concept by a sign which denotes it NOTE In terminology work three types of designations are distinguished: symbols, appellations, (a.k.a. names), and terms.	designation	02	représentation d'un concept par un signe qui le dénomme NOTE Dans le travail terminologique, on distingue trois types de désignation les symboles, les appellations (c.-à-d. des noms) et les termes.
3.035	ISO/IEC 10181-2:1996 (3.11)	distinguishing identifier	99	**data** that unambiguously distinguishes an **entity** in the **authentication process**	identificateur distinctif	01	**données** qui différencient sans ambiguïté une **entité** dans le **processus d'authentification**

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.036	ISO/IEC 21987-1 (3.036)	eBusiness (in learning transaction)	99	**learning transaction**, involving the making of **commitments**, in a defined **collaboration space**, among **Persons** using their **IT systems**, according to **Open-edi standards** NOTE 1 eBusiness can be conducted on both a for-profit and not-for-profit basis. NOTE 2 A key distinguishing aspect of eBusiness is that it involves the making of commitment(s) of any kind among the Persons in support of a mutually agreed upon goal, involving their IT systems, and doing so through the use of EDI (using a variety of communication networks including the Internet). NOTE 3 eBusiness includes various application areas such as “e-commerce”, “e-administration”, “e-logistics”, “e-government”, “e-medicine”, “e-learning”, etc. NOTE 4 The equivalent French language term for “eBusiness” is always presented in its plural form. NOTE 5 Adapted from ISO/IEC 15944-7.	eAffaires (dans une transaction d’apprentissage)	02	**transaction d’apprentissage**, impliquant la prise des **engagements**, dans une **espace de collaboration**, entre **Personnes** utilisant leurs **systèmes TI**, par application des **normes** d’**EDI-ouvert** NOTE 1 On peut entreprendre des eAffaires dans un but lucratif on non. NOTE 2 Une caractéristique clé des eAffaires est l’implication d’engagement(s) de toute(s) sorte(s) entre les Personnes qui poursuivent un but convenu mutuellement et impliquant leurs systèmes TI, et ce faisant, grâce au recours à l’EDI (en utilisant une variété de réseaux de communication dont l’Internet). NOTE 3 Les eAffaires incluent divers secteurs d’applications tels que le « e-commerce »commerce électronique, « e-administration », « e-logistique », « e-gouvernement », « e-médicine », e-apprentissage », etc. NOTE 4 Le terme français « eAffaires » s’emploie toujours au pluriel. NOTE 5 Adapté de l’ISO/CEI 15944-7.
3.037	ISO/IEC 15944-2:2006 (3.32)	electronic address	99	**address** used in a recognized electronic addressing scheme, (e.g., telephone, telex, IP, etc.), to which **recorded information** item(s) and/or business object(s) can be sent to or received from a Contact	adresse électronique	02	**adresse** utilisée dans un système d’adressage électronique reconnu (par ex. le téléphone, le télex, l’IP, etc.) à laquelle un Contact peut envoyer ou recevoir un (ou des) article(s) d’**information enregistrée** et/ou un (ou des) objet(s) d’affaires
3.038	ISO/IEC 14662:2004 (3.8)	Electronic Data Interchange (EDI)	99	automated exchange of any predefined and structured **data** for **business** purposes among information systems of two or more **Persons** NOTE This definition includes all categories of electronic **learning transaction**s.	Échange de Données Informatisé (EDI)	01	échange automatisé de **données** structurées et prédéfinies pour traiter des **affaires** entre les systèmes d'information de deux ou plusieurs **Personnes**. NOTE Cette définition inclut toutes les catégories de transactions d’affaires électroniques.
3.039	ISO/IEC 2382-17:1999 (17.02.05)	entity	99	any concrete or abstract thing that exists, did exist, or might exist, including associations among these things EXAMPLE A Person, object, event, idea, process, etc. NOTE An entity exists whether data about it are available or not.	entité	02	tout objet ou association d'objets, concret ou abstrait, existant, ayant existé ou pouvant exister EXEMPLE Personne, événement, idée, processus, etc. NOTE Une entité existe que l'on dispose de données à son sujet ou non.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.040	ISO/IEC 9788-1:1997 (3.3.1)	entity authentication	99	corroboration that the **entity** is the one claimed	authentification de l'entité	02	corroboration que l'**entité** est bien celle qui est revendiquée
3.041	ISO/IEC 15944-5:2008 (3.49)	exchange code set	99	set of **ID codes** identified in a **coded domain** as being suitable for information exchange as shareable **data** EXAMPLE The 3 numeric, 2-alpha and 3-alpha code sets in ISO 3166-1.	ensemble de codes d'échange	01	ensemble de **codes ID** identifié dans un **domaine codé** comme convenant à l'échange d'information en tant que **données** partageables EXEMPLE L'ensemble des 3 codes numériques, alphabétiques à 2 lettres et alphabétiques à 3 lettres, dans l'ISO 3166-1.
3.042	ISO/IEC 29187-1 (3.042)	external constraint (in LET privacy protection)	99	**constraint** which takes precedence over **internal constraints** in a **learning transaction**, i.e., is external to those agreed upon by the parties to a **learning transaction** NOTE 1 Normally external constraint is created by law, regulation, orders, treaties, conventions or similar instruments. NOTE 2 Other sources of external constraints are those of a sectoral nature, those which pertain to a particular jurisdictional domain or a mutually agreed to common business conventions, (e.g., INCOTERMS, exchanges, etc.). NOTE 3 External constraints can apply to the nature of the good, service and/or right provided in a learning transaction NOTE 4 External constraints can demand that a party to a learning transaction meet specific requirements of a particular role. EXAMPLE 1 Only a qualified medical doctor may issue a prescription for a controlled drug. EXAMPLE 2 Only an accredited share dealer may place transactions on the New York Stock Exchange. EXAMPLE 3 Hazardous wastes may only be conveyed by a licensed enterprise. NOTE 5 Where the information bundles (IBs), including their Semantic Components (SCs) of a learning transaction are also to form the whole of a learning transaction, (e.g., for legal or audit purposes), all constraints must be recorded. EXAMPLE There may be a legal or audit requirement to maintain the complete set of recorded information pertaining to a learning transaction, i.e., as the information bundles exchanged, as a "record".	contrainte externe (dans la protection de la vie privée concernant l'AÉF)	02	**contrainte** qui l'emporte sur les **contraintes internes** dans une **transaction d'apprentissage** c.-à-d. qui est externe à celles convenues entre les parties dans une **transaction d'apprentissage** NOTE 1 Normalement, les contraintes externes découlent des lois, règlements, décrets, traités, conventions, ou autres instruments semblables. NOTE 2 D'autres sources de contraintes externes sont de nature sectorielle, qui relèvent d'une juridiction particulière, ou de conventions d'affaires convenues mutuellement, (par ex. INCOTERMS, les échanges, etc.). NOTE 3 Des contraintes externes peuvent s'exercer sur la nature des biens, des services, et/ou au droit accordé dans une transaction d'apprentissage. NOTE 4 Des contraintes externes peuvent exiger qu'une partie, dans une transaction d'apprentissage réponde aux exigences spécifiques d'un rôle. EXEMPLE 1 Seul un médecin diplômé peut prescrire une ordonnance pour un médicament contrôlé. EXEMPLE 2 Seul un courtier en actions accrédité peut effectuer des transactions à la bourse de New York. EXEMPLE 3 Seule une entreprise attitrée peut transporter des déchets dangereux. NOTE 5 Lorsque les faisceaux d'information, y compris leurs composantes sémantiques, d'une transaction d'apprentissage constituent l'ensemble d'une transaction d'apprentissage (par ex. à des fins juridiques ou comptables), toutes les contraintes doivent être enregistrées. EXEMPLE Il peut exister une exigence juridique ou comptable de conserver la totalité des documents enregistrés relatifs à une transaction d'apprentissage, c.-à-d. les faisceaux d'information échangés, comme un «enregistrement».

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 6 A minimum external constraint applicable to a learning transaction often requires one to differentiate whether the Person, i.e., that is a party to a learning transaction, is an "individual", "organization", or "public administration". For example, privacy rights apply only to a Person as an "individual". NOTE 7 Adapted from ISO/IEC 15944-1.			NOTE 6 Une contrainte externe minimum applicable à une transaction d' d'apprentissage exige souvent de distinguer si une Personne, c.-à-d. une partie dans une transaction d'apprentissage, est un «individu», une «organisation» ou une «administration publique». Par ex., les droits de protection de la vie privée ne s'appliquent qu'à une Personne en tant qu' «individu». NOTE 7 Adapté de l'ISO/CEI 15944-1.
3.043	ISO/IEC 14662:2010 (3.9)	Formal Description Technique (FDT)	99	specification method based on a description language using rigorous and **unambiguous rules** both with respect to developing expressions in the language (formal syntax) and interpreting the meaning of these expressions (formal semantics)	Technique de description formelle (FDT)	02	méthode de spécification fondée sur un langage de spécification faisant appel à des **règles** rigoureuses et **non ambiguës** tant pour le développement d'expressions dans le langage (syntaxe formelle) que pour l'interprétation de la signification de ces expressions (sémantique formelle)
3.044	ISO/IEC 14662:2010 (3.10)	Functional Service View (FSV)	99	perspective of **business** transactions limited to those information technology interoperability aspects of **IT Systems** needed to support the execution of Open-edi transactions	Vue fonctionnelle des services (FSV)	02	vue perspective sur les transactions d'**affaires**, restreinte à ceux des aspects relatifs au fonctionnement informatique coopératif entre **systèmes d'information** qui sont nécessaires à l'exécution des transactions d'EDI-ouvert
3.045	ISO/IEC 15944-2:2006 (3.35)	Human Interface Equivalent (HIE)	99	representation of the **unambiguous** and IT-enabled semantics of an IT **interface equivalent**, often the **ID code** of a coded domain (or a **composite identifier**), in a formalized manner suitable for communication to and understanding by humans NOTE 1 Human interface equivalents can be linguistic or non-linguistic in nature but their semantics remains the same although their representations may vary. NOTE 2 In most cases there will be multiple Human Interface Equivalent representations as required to meet localization requirements, i.e. those of a linguistic nature, jurisdictional nature, and/or sectoral nature. NOTE 3 Human Interface Equivalents include representations in various forms or formats, (e.g., in addition to written text those of an audio, symbol (and icon) nature, glyphs, image, etc.).	Équivalent d'interface humaine (ÉIH)	01	représentation de la sémantique **non-ambigüe** et habilitée TI d'une équivalente **interface TI**, souvent le **code ID** d'un **domaine codé** (ou d'un **identificateur composite**), d'une manière formalisée qui convient à la communication et qui est compréhensible par les humains NOTE 1 Les équivalents d'interface humaine peuvent être de nature linguistique on non, mais leur sémantique reste la même bien que leurs représentations puissent varier. NOTE 2 Dans la plupart des cas, il y aura des représentations d'équivalents d'interface humaine multiples selon les besoins pour répondre aux exigences en matière de localisation, c.-à-.d. ceux de nature linguistique, juridictionnelle et/ou sectorielle. NOTE 3 Les équivalents d'interface humaine comprennent les représentations sous formes et formats différents (par ex. en plus du texte écrit, l'audio, les symboles, les icônes, les glyphes, les images, etc.).
3.046	ISO/IEC 15944-2:2006 (3.36)	IB Identifier	99	unique, linguistically neutral, unambiguous referenceable identifier for an Information Bundle	identificateur IB	01	identificateur d'un Faisceau d'informations unique, linguistiquement neutre et référençable de façon non-ambigüe

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.047	ISO/IEC 15944-2:2006 (3.37)	ID Code	99	**identifier** assigned by the coded domain **Source Authority (cdSA)** to a member of a **coded domain ID** NOTE 1 ID codes must be unique within the Registration Schema of that coded domain. NOTE 2 Associated with an ID code in a coded domain can be: (a) one or more equivalent codes; (b) one or more equivalent representations, especially those in the form of human equivalent (linguistic) expressions. NOTE 3 Where an entity as a member of a coded domain is allowed to have more than one ID code, i.e., as equivalent codes (possibly including names), one of these must be specified as the pivot ID code. NOTE 4 A coded domain may contain ID codes pertaining to entities which are not members as peer entities, i.e., have the same properties and behaviours, such as ID codes which pertain to predefined conditions other than member entities. If this is the case, the rules governing such exceptions must be predefined and explicitly stated. EXAMPLE Common examples include: (1) the use of an ID code "0" (or "00", etc.), for “Other”; (2) the use of an ID code "9" (or "99") for “Not Applicable”; (3) the use of “8” (or “98”) for “Not Known”; if required, (4) the pre-reservation of a series or set of ID codes for use for "user extensions". NOTE 5 In UML modeling notation, an ID code is viewed as an instance of an object class.	code ID	01	**identificateur** attribué par l'**Autorité de source** du **domaine codé (cdSA)** à un membre d'une **ID de domaine codé** NOTE 1 Les codes ID doivent être uniques dans le Schéma d'enregistrement de ce domaine codé. NOTE 2 On peut rattacher à un code ID dans un domaine codé : (a) un ou plusieurs codes équivalents; (b) une ou plusieurs représentations équivalentes; en particulier ceux et celles qui sont sous forme d'expressions (linguistiques) équivalentes humaines. NOTE 3 Lorsque l'on permet à une entité en tant que membre d'un domaine codé d'avoir plus d'un code ID, c.-à.-d. comme codes équivalents, l'un de ces codes doit être spécifié comme code ID pivot. NOTE 4 Un domaine codé peut contenir des codes ID relatifs aux entités qui ne sont pas membres à titre d'entités paires, c.-à.-d. ont les mêmes propriétés et comportements, tels que les codes ID relatifs à des conditions prédéfinies autres que celles des entités membres. Dans ce cas, les règles régissant de telles exceptions doivent être prédéfinies et énoncées explicitement. EXEMPLE Comme exemples communs, on trouve : (1) l'utilisation d'un code ID « 0 » (ou « 00 », etc.) pour « Autres »; l'utilisation d'un code ID « 9 » (ou « 99 ») pour « Sans objet »; l'utilisation du « 8 » (ou « 88 ») pour « non connu » ; et/ou, si nécessaire, (4) la pré réservation d'une série ou d'ensemble de codes ID pour usage dans les « extensions utilisateur ». NOTE 5 Dans la notation de modélisation UML, un code ID est considéré comme instance de classe d'objet.
3.048	ISO/IEC 15944-1:2011 (3.26)	identification	99	*rule*-based **process**, explicitly stated, involving the use of one or more **attributes**, i.e., **data elements**, whose value (or combination of values) are used to identify uniquely the occurrence or existence of a specified **entity**	identification	02	processus basé sur des **règles**, énoncées explicitement, impliquant l'utilisation d'un ou plusieurs **attributs**, c.-à-d. des **éléments de données**, dont la valeur (ou une combinaison de valeurs) sert à identifier de façon unique l'occurrence ou l'existence d'une **entité** spécifiée

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.049	ISO/IEC 29187-1 (3.049)	identifier (in learning transaction)	99	**unambiguous**, unique and a linguistically neutral value, resulting from the application of a **rule**-based **identification process** NOTE 1 Identifiers must be unique within the identification scheme of the issuing authority. NOTE 2 An identifier is a linguistically independent sequence of characters capable of uniquely and permanently identifying that with which it is associated. {See ISO 19135:2005 (4.1.5)} NOTE 3 Adapted from ISO/IEC 15944-1.	identificateur (dans une transaction d'apprentissage)	01	valeur **non-ambiguë** et linguistiquement neutre, résultant de l'application d'un **processus** d'**identification** à base de **règles** NOTE 1 Les identificateurs doivent être uniques dans le système d'identification de l'autorité émettrice. NOTE 2 Un identificateur est une séquence de caractères linguistiquement indépendante capable d'identifier de façon unique et permanente ce à quoi il est associé. {voir ISO 19135:2005 (4.1.5)} NOTE 3 Adapté de l'ISO/CEI 15944-1.
3.050	ISO/IEC 15944-1:20011 (3.28)	individual	99	**Person** who is a human being, i.e., a natural Person, who acts as a distinct indivisible **entity** or is considered as such	individu	01	**Personne** qui est un être humain, c.-à-d. une personne physique, qui agit à titre d'**entité** indivisible distincte ou qui est considérée comme telle
3.051	ISO/IEC 29187-1 (3.051)	individual accessibility (in LET privacy protection)	99	set of **external constraints** of a **jurisdictional domain** as rights of an **individual** with disabilities to be able to use IT systems at the human, i.e., user, interface and the concomitant obligation of a **LET provider** to provide such adaptive technologies NOTE 1 Although "accessibility" typically addresses users who have a disability, the concept is not limited to disability issues. EXAMPLE Examples of disabilities in the form of functional and cognitive limitations include: - people who are blind; - people with low vision; - people with colour blindness; - people who are hard of hearing or deaf, i.e., are hearing impaired; - people with physical disabilities; - people with language or cognitive disabilities. NOTE 2 Adapted from ISO/IEC 15944-5.	accessibilité individuelle (dans la protection de la vie privée concernant l'AÉF)	02	ensemble de **contraintes externes** d'un **domaine juridictionnel** comme droits d'un **individu** atteint de déficience d'être capable d'utiliser des systèmes TI au niveau de l'interface humaine, c.-à.-d. utilisateur, et l'obligation concomitante d'un **fournisseur d'AÉF** d'offrir ce type de technologies adaptatives NOTE 1 Bien que l'« accessibilité » s'adresse typiquement aux utilisateurs qui ont une déficience, le concept ne se limite pas aux questions de déficience. EXEMPLE Comme exemples de déficiences sous formes de limitations fonctionnelles et cognitives, on trouve : - les personnes aveugles; - les personnes à basse vision; - les personnes atteintes d'achromatopsie; - les personnes sourdes ou ayant une déficience auditive; - les personnes atteintes de déficience physique; - les personnes atteintes de déficience linguistique ou cognitive. NOTE 2 Adapté de l'ISO/CEI 15944-5.
3.052	ISO/IEC 29187-1 (3.052)	individual anonymity (in LET privacy protection)	99	state of not knowing the identity or no having any recording of **personal information** on or about an **individual** as a **learner** by the **LET provider** or **regulator**, (or any other party) to a **learning transaction** NOTE Adapted from ISO/IEC 15944-8.	anonymité individuelle (dans la protection de la vie privée concernant l'AÉF)	02	état d'indisponibilité de l'identité ou de l'enregistrement de renseignements personnels sur (ou au sujet d') un **individu** comme **apprenant**, constatée par le **fournisseur d'AÉF** ou une **autorité de réglementation** (ou tout autre tiers) partie prenante d'une **transaction d'apprentissage** NOTE Adapté de l'ISO/CEI 15944-8.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.053	ISO/IEC 29187-1 (3.053)	individual authentication (in LET privacy protection)	99	provision of the assurance of a r**ecognized individual identity (rii)** sufficient for the purpose of the **learning transaction** NOTE Adapted from ISO/IEC 15944-8.	identification individuelle (dans la protection de la vie privée concernant l'AÈF)	02	présentation d'une garantie concernant une **identification individuelle reconnue** et suffisante pour l'utilisation dans une **transaction d'apprentissage** NOTE Adapté de l'ISO/CEI 15944-8.
3.054	ISO/IEC 29187-1 (3.054)	individual identity (ii) (in LET privacy protection)	99	**Person identity** of an **individual**, i.e., an individual identity, consisting of the combination of the **persona** information and **identifier** used by an **individual** in a **learning transaction**, i.e., the making of any kind of **commitment** NOTE Adapted from ISO/IEC 15944-8.	identité individuelle (dans la protection de la vie privée concernant l'AÈF)	02	**identité d'une Personne** d'un **individu**, c.-à.-d., identité individuelle, consistant en la combinaison d'information sur la **persona** et l'**identificateur** utilisée par un **individu** dans une **transaction d'apprentissage**, c.-à.-d. la prise de toute forme d'**engagement** NOTE Adapté de l'ISO/CEI 15944-8.
3.055	ISO/IEC 29187-1 3.055	individual learner	99	learner who participates as an **individual** in a **learning transaction**	apprenant individuel	01	apprenant qui participe à titre d'**individu** dans une **transaction d'apprentissage**
3.056	ISO/IEC 15944-8 (3.060)	individual persona Registration Schema (ipRS)	99	**persona Registration Schema (pRS)** where the **persona** is, or includes, that of an **individual** being registered NOTE 1 Where an persona Registration Schema includes persona of sub-types of Persons, i.e., individuals, organizations, and/or, public administrations, those which pertain to individuals shall be identified as such because public policy as external constraints apply including those of a privacy protection requirements nature. NOTE 2 In a individual persona Registration Schema, one shall state whether or not a truncated name, i.e. registered persona, of the individual, is allowed or mandatory, and if so the ipRS shall explicitly state the rules governing the formation of the same.	schéma d'enregistrement d'une persona individuelle (ipRS)	01	**schéma d'enregistrement d'une persona (pRS)** selon lequel la **persona** est, ou inclut, celle d'un **individu** en cours d'enregistrement NOTE1 Lorsque le Schéma d'enregistrement d'une persona inclut des persona de sous-catégories de personnes, c.-à.-d. des individus, des organisations, et/ou des administrations publiques, les éléments précités qui se réfèrent à des individus doivent être identifiés comme tels, car les politiques publiques en tant que contraintes externes s'appliquent alors, y compris celles de nature des exigences de protection de la vie privée. NOTE 2 Dans un schéma d'enregistrement d'une persona individuelle (ipRS), on est tenu de préciser si un nom complet ou abrégé (c.-à.-d. la persona enregistrée) est autorisé et obligatoire, et en ce cas, l'ipRS doit définir clairement les règles applicables à sa formation.
3.057	ISO/IEC 14662:2010 (3.11)	Information Bundle (IB)	99	formal description of the semantics of the **recorded information** to be exchanged by **Open-edi Parties** playing **roles** in an **Open-edi scenario**	Faisceau d'informations (IB)	01	description formelle de la valeur sémantique des **informations enregistrées** échangées entre **partenaires** d'**EDI-ouvert** jouant un **rôle** dans un **scénario d'EDI-ouvert**

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.058	ISO/IEC 15944-8 (3.062)	information law	99	any law, regulation, policy, or code (or any part thereof) that requires the creation, receipt, collection, description or listing, production, retrieval, submission, retention, storage, preservation or destruction of **recorded information**, and/or that places conditions on the access and use, confidentiality, privacy, integrity, accountabilities, continuity and availability of the processing, reproduction, distribution, transmission, sale, sharing or other handling of **recorded information**	droit de l'information	02	toute loi ou règle, politique ou code (ou toute partie de ces supports) qui requièrent la création, la conservation, la collection, la description ou la mise en liste, la production, la recherche, la fourniture, la rétention, le stockage la préservation ou la destruction d'**information enregistrée** et /ou les lieux, conditions de l'accès à l'usage, la confidentialité, la protection personnelle, l'intégrité, la communication, la continuité et la disponibilité du traite la reproduction, de la transmission, de la vente du partage et de toute autre opération sur l'**information enregistrée**.
3.059	ISO/IEC 14662:2010 (3.12)	Information Processing Domain (IPD)	99	**Information Technology System** which includes at least either a **Decision Making Application (DMA)** and/or one of the components of an Open-edi Support Infrastructure (or both), and acts/executes on behalf of an **Open-edi Party** (either directly or under a delegated authority)	Domaine de traitement de l'information (IPD)	01	**système d'information** comprenant au moins une **Application à pouvoir (DMA) de décision** ou un des composants de l'infrastructure de support d'EDI-ouvert (ou les deux), agissant ou fonctionnant au nom d'un **partenaire d'EDI-ouvert** (directement ou par délégation d'autorité)
3.060	ISO/IEC 14662:2010 (3.13)	Information Technology System (IT System)	99	set of one or more computers, associated software, peripherals, terminals, human operations, physical **processes**, information transfer means, that form an autonomous whole, capable of performing information processing and/or information transfer	système d'information (IT System)	01	ensemble constitué d'un ou de plusieurs ordinateurs, avec leurs logiciels associés, de périphériques, de terminaux, d'opérateurs humains, de **processus** physiques et de moyens de transfert d'information, formant un tout autonome capable de traiter l'information et/ou de la transmettre
3.061	ISO/IEC 29187-1 (3.061)	internal constraint (in LET privacy protection)	99	**constraint** which forms part of the **commitment**(s) mutually agreed to among the parties to a **learning transaction** NOTE 1 Internal constraints are self-imposed. They provide a simplified view for modelling and re-use of scenario components of a learning transaction for which there are no external constraints or restrictions to the nature of the conduct of a learning transaction other than those mutually agreed to by the individual learner and LET provider NOTE 2 Adapted from ISO/IEC 15944-1.	contrainte interne (dans la protection de la vie privée concernant l'AÉF)	02	**contrainte** qui fait partie de l'**engagement** convenu mutuellement entre les parties d'une **transaction d'apprentissage** NOTE 1 Les contraintes internes sont volontaires. Elles présentent une vue simplifiée de modélisation et de réutilisation des composantes de scénario d'une transaction d'apprentissage sans contraintes ou restrictions externes quant à la conduite d'une transaction d'apprentissage autres que celles convenues mutuellement entre l'apprenant individuel et le fournisseur d'AÉF. NOTE 2 Adapté de l'ISO/CEI 15944-1.
3.062	ISO/IEC 29187-1 (3.062)	IT-enablement (in LET privacy protection)	99	transformation of a current **standard** used in **learning transaction**s, (e.g., **coded domains**), from a manual to computational perspective so as to be able to support **commitment** exchange and **computational integrity** NOTE Adapted from ISO/IEC 15944-8.	habilitation TI (dans la protection de la vie privée concernant l'AÉF)	02	transformation des **normes** actuelles utilisées dans la **transaction d'apprentissage** (par exemple, les **domaines codés**) de mode manuel en mode informatique, afin de pouvoir assurer un échange d'**engagements** et une **intégrité informatique** NOTE Adapté de l'ISO/CEI 15944-8.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.063	ISO/IEC 291871-(3.063)	jurisdictional domain (in LET privacy protection)	99	jurisdiction, recognized in law as a distinct legal and/or regulatory framework, which is a source of **external constraints** on **Persons**, their behaviour and the making of **commitments** among **Persons** including any aspect of a **learning transaction** NOTE 1 The pivot jurisdictional domain is a United Nations (UN) recognized member state. From a legal and sovereignty perspective they are considered "peer" entities. Each UN member state, (a.k.a. country) may have sub-administrative divisions as recognized jurisdictional domains, (e.g., provinces, territories, cantons, länder, etc.), as decided by that UN member state. NOTE 2 Jurisdictional domains can combine to form new jurisdictional domains, (e.g., through bilateral, multilateral and/or international treaties). EXAMPLE Included here, for example, are the European Union (EU), NAFTA, WTO, WCO, ICAO, WHO, Red Cross, the ISO, the IEC, the ITU, etc. NOTE 3 Several levels and categories of jurisdictional domains may exist within a jurisdictional domain. NOTE 4 A jurisdictional domain may impact aspects of the commitment(s) made as part of a **learning transaction** including those pertaining to the making, selling, transfer of goods, services and/or rights (and resulting liabilities) and associated information. This is independent of whether such interchange of commitments are conducted on a for-profit or not-for-profit basis and/or include monetary values. NOTE 5 Laws, regulations, directives, etc., issued by a jurisdictional domain are considered as parts of that jurisdictional domain and are the primary sources of external constraints on **learning transaction**s. Note 6 Adapted form ISO/IEC 15944-5.	domaine juridictionnel (dans la protection de la vie privée concernant l'AÈF)	01	juridiction, reconnue par la loi comme cadre juridique distinct et/ou de réglementation, qui est une source de **contraintes externes** pour les **Personnes**, leur comportement et la prise d'**engagements** entre les **Personnes**, y compris tout aspect d'une **transaction d'apprentissage** NOTE 1 Le domaine juridictionnel pivot est un état membre reconnu par les Nations unies (ONU). Dans une perspective juridique et de souveraineté, tous les états sont considérés comme des entités « paires ». Chaque état membre de l'ONU (alias pays) peut avoir des subdivisions administratives comme domaines juridictionnels reconnus (par ex. provinces, territoires, cantons, länder, etc.), tel que décidé par cet état membre de l'ONU. NOTE 2 Des domaines juridictionnels peuvent être combinés pour former de nouveaux domaines juridictionnels (par ex., grâce à des traités bilatéraux, multilatéraux et/ou internationaux). EXEMPLES l'Union européenne (UE), l'ALENA, l'OMC, l'OMD, l'OACI, l'OMS, la Croix-Rouge, l'ISO, la CEI, l'UIT, etc. NOTES 3 Plusieurs niveaux et catégories de domaines juridictionnels peuvent exister à l'intérieur d'un domaine juridictionnel. NOTE 4 Un domaine juridictionnel peut avoir des répercussions sur des aspects des engagements pris dans le cadre de transactions d'apprentissage, compris celles qui ont trait à la fabrication, la dispensation, la vente et le transfert de biens, de services et/ou de droits (et des responsabilités qui en résultent), et l'information connexe. Ceci indépendamment du fait que de tels échanges d'engagements peuvent s'effectuer dans un (ou sans) but lucratif et/ou inclure des valeurs monétaires. NOTE 5 Les lois, règlements, directives, etc., promulgués par un domaine juridictionnel sont considérés comme faisant partie de ce domaine juridictionnel et sont les sources principales de contraintes externes exercées sur les transactions d'apprentissage. NOTE 6 Adapté de l'ISO/CEI 15944-5.
3.064	ISO/IEC 15944-2:2006 (3.47)	jurisdictional domain identifier	99	**ID code** of a **jurisdictional domain** as recognized for use by peer **jurisdictional domains** within a system of mutual recognition	identificateur de domaine juridictionnel	01	**code ID** d'un d**omaine juridictionnel reconnu** pour utilisation par **des domaines juridictionnels** pairs dans un système de reconnaissance mutuelle

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.065	ISO 5127-1:2001 (1.1.2.01)	language	99	system of signs for communication, usually consisting of a **vocabulary** and **rules** NOTE In this part of ISO/IEC 21987, language refers to natural languages or special languages, but not "programming languages" or "artificial languages".	langue	02	système de signes de communication compose habituellement d'un **vocabulaire** et de **règles** NOTE Dans la présente norme, la langue se réfère aux langues naturelles ou aux langues de spécialité, mais pas aux « langages de programmation » ou « langages artificiels ».
3.066	ISO 639-2:1998 (3.2)	language code	99	combination of **characters** used to represent a **language** or **languages** NOTE In ISO/IEC 29187, the ISO 639-2/T (terminology) three alpha-codes, shall be used.	codet de langue	01	combinaison de **caractères** utilisées pour représenter une **langue** ou des **langues** NOTE Dans la présente norme ISO/IEC 29187, le code alpha trois de l'ISO 639-2/T (terminologie) doit être utilisé.
3.067	ISO/IEC 29187-1 (3.067)	learning collaboration space	99	learning activity space where exchanges of **recorded information**, valued resources, and related activities is viewed independently and not from the perspective of any party to a **learning transaction** NOTE Adapted from ISO/IEC 15944-4.	espace collaboratif d'apprentissage	01	espace d'activités d'apprentissage où un échange de **données enregistrées**, de ressources valorisées, et toutes activités connexes, est individualise comme tel, indépendamment de l'optique de toute partie prenante à la **transaction d'apprentissage** NOTE Adapté de l'ISO/CEI 15944-4.
3.068	ISO/IEC 29187-1 (3.068)	learning event	99	occurrence in time that partners to a **learning transaction** wish to monitor or control NOTE 1 Learning events are the workflow tasks that learning partners need to accomplish to complete a learning transaction among themselves. As learning events occur, they cause a learning transaction to move through its various phases of planning, identification, negotiation, actualization, and post-actualization. NOTE 2 Occurrences in time can either be: (1) internal as mutually agreed to among the parties to a learning transaction; and/or, (2) reference some common publicly available and recognized date/time referencing schema, (e.g., one based on using the ISO 8601 and/or ISO 19135 standards). NOTE 3 Adapted from ISO/IEC 15944-4.	évènement d'apprentissage	01	évènement daté que des partenaires d'une **transaction d'apprentissage** conviennent ensemble de guider ou de contrôler NOTE 1 Les évènements d'apprentissage sont les séries de tâches que les partenaires d'une formation doivent accomplir pour assurer ensemble une transaction d'apprentissage. Au fur et à mesure que les évènements d'apprentissage se produisent, ils initient une transaction d'apprentissage qui suivra les étapes prévues de phasage, d'identification, de négociation, d'actualisation et de recadrage. NOTE 2 La réalisation dans le temps des évènements d'apprentissage peut avoir pour origine, alternativement, soit : (1) des causes internes, convenues d'un commun accord entre les parties d'une transaction d'apprentissage; et/ou, (2) la prise en compte d'un corps de règles de datation et d'horaire qui soit reconnu et d'accès public (fondé par ex., sur l'application des normes ISO 8601 et/ou ISO 19135). NOTE 3 Adapté de l'ISO/CEI 15944-4.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.069	ISO/IEC 29187-1 (3.069)	learning object	99	**unambiguously** identified, specified, referenceable, registered and re-useable **Open-edi scenario** or **scenario component** of a **learning transaction** NOTE 1 As an “object”, a “learning object” exists only in the context of a **learning transaction**. NOTE 2 Adapted from ISO/IEC 15944-2.	objet d’apprentissage	01	**scénario d'EDI–ouvert** identifié, spécifié, référençable, enregistré et réutilisable sans **ambiguïté**, ou **composante de scénario** d’une **transaction d’apprentissage**. NOTE 1 En tant qu’ « objet », un « objet d’apprentissage » n’existe que dans le contexte d’une transaction d’apprentissage. NOTE 2 Adapté de l’ISO/CEI 15944-2.
3.070	ISO/IEC 29187-1 (3.070)	learning transaction		predefined set of activities and/or **processes** among **Persons** which is initiated by a **Person** to accomplish an explicitly stated learning goal and terminated upon recognition of one of the agreed conclusions by all the involved **Persons** although some of the recognition may be implicit NOTE 1 A learning transaction may be internal constraints-based or external constraints-based. A primary example of an external constraint-based learning transaction is that of jurisdictional domains governing minimum levels of schooling, (e.g., K-12). NOTE 2 A learning transaction can be on a for-a-fee or for-free basis. NOTE 3 A LET provider can offer a learning transaction and operate on either a for-profit or not-for-profit basis. NOTE 4 Adapted from ISO/IEC 14662.	transaction d’apprentissage	02	ensemble prédéterminé d'activités et/ou de **processus** menés par une **Personne** pour atteindre un objectif d’apprentissage énoncé explicitement terminé lorsqu'est observée une des conclusions convenues par toutes les **Personnes** prenantes, bien que cette observation puisse être partiellement implicite NOTE 1 Une transaction d’apprentissage peut être fondée sur des règles et contraintes externes ou internes. Un exemple évident d'une transaction d’apprentissage fondée sur des contraintes externes est celui des règles publiques applicables à la scolarisation (voir K-12). NOTE 2 Une transaction d’apprentissage peut être gratuite ou payante NOTE 3 Un fournisseur d’apprentissage peut offrir une transaction d’apprentissage en opérant tantôt sur une base d'entreprise ou sur une base publique NOTE 4 Adapté de l’ISO/CEI 14662.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.071	ISO/IEC 29187-1 (3.071)	learning transaction identifier (LTI)	99	**identifier** assigned by a **LET provider** or a **regulator** to an instantiated **learning transaction** among the **Persons** involved NOTE 1 The identifier assigned by the LET provider or regulator shall have the properties and behaviours of an “identifier (in a learning transaction)”. NOTE 2 As an identifier (in a learning transaction), a LTI serves as the unique common identifier for all Persons involved for the identification, referencing, retrieval of recorded information, etc., pertaining to the commitments made and the resulting actualization (and post-actualization) of the learning transaction agreed to. NOTE 3 A learning transaction identifier can be assigned at any time during the planning, identification or negotiation phases but shall be assigned at least prior to the start or during the actualization phase. NOTE 4 As and where required by the applicable jurisdictional domain(s), the recorded information associated with the learning transaction identifier (LTI) may well require the LET provider to include other identifiers, (e.g., from a value-added good or service tax, etc., perspective) as assigned by the applicable jurisdictional domain(s). NOTE 4 Adapted from ISO/IEC 15944-5.	identificateur de transaction d’apprentissage (LTI)	01	**identificateur** attribué par un **fournisseur d’AÉF** ou une **autorité de réglementation** à une **transaction d’apprentissage** instanciée parmi les **Personnes** concernées NOTE 1 L’identificateur attribué par l’opérateur ou l’autorité de régulation doit avoir les propriétés et le comportement d’un « identificateur" (dans une transaction d’apprentissage). NOTE 2 En tant qu’identificateur (dans une transaction d’apprentissage, un LTI est utilisé comme identificateur commun unique pour toutes les Personnes concernées dans l’identification, le référencement, l’extraction d’information enregistrée, etc., relatifs aux engagements pris et à l’actualisation (et la reformulation) de la transaction d’apprentissage qui s'y rapporte. NOTE 3 Un identificateur de transaction d’apprentissage (LTI) peut être attribué à n’importe quel moment durant les phases de planification, d’identification ou de négociation, mais doit être attribué au moins avant le début ou durant la phase d’actualisation. NOTE 4 Selon les besoins et le lieu du (des) domaine(s) juridictionnel(s) applicable(s), l’information enregistrée rattachée à l’identificateur de transaction d’apprentissage (LTI) peut obliger le fournisseur d’apprentissage à inclure d'autres éléments d'identification requis par la règlementation applicable (par ex. une taxe sur le produit ou service de valeur ajoutée, etc.). NOTE 5 Adapté de l’ISO/CEI 15944-5.
3.072	ISO/IEC 29187-1 (3.072)	legally recognized individual identity (LRII)	99	**recognized individual identity (rii)** which includes the use of a **recognized individual name (RIN)** and the associated **identifier,** i.e., **ID code**, assigned as part of the **personal information** for that **individual** in the **individual persona Registration Schema (ipRS)**	identité individuelle reconnue légalement (LRII)	02	**identité individuelle reconnue (rii)** qui inclut l’utilisation d’un **nom individuel reconnu (NIR)** et de l’identificateur connexe, c.-à.-d. le **code ID**, attribué comme partie des **renseignement personnels** sur cet **individu** dans le **Schéma d’enregistrement**
3.073	ISO./IEC 29187-1 (3.073)	legally recognized individual persona Registration Schema (LipRS)	99	**individual persona Registration Schema (ipRS)** which has legal status and is so recognized in a **jurisdictional domain** as being able to register a **recognized individual name (RIN)** and unique **identifier** associated with such a registration	Schéma d’enregistrement d’une persona individuelle reconnu légalement (LipRS)	01	**Schéma d’enregistrement d’une persona individuelle (ipRS)** qui a un statut juridique et est ainsi reconnu dans un **domaine juridictionnel** comme étant capable d’enregistrer un **nom individuel reconnu (NIR)** et un **identificateur** unique associé à un tel enregistrement

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.074	ISO/IEC 15944-5:2008 (3.71)	legally recognized language (LRL)	99	**natural language** which has status (other than an **official language** or **de facto language**) in a **jurisdictional domain** as stated in an act, regulation, or other legal instrument, which grants a community of people (or its i**ndividuals**) the right to use that **natural language** in the context stipulated by the legal instrument(s) NOTE The LRL can be specified through either: (a) the) the identification of a language by the name used; or, (b) the identification of a people and thus their language(s). EXAMPLE In addition to acts and regulations, legal instruments include self-government agreements, land claim settlements, court decisions, jurisprudence, etc.	langue reconnue légalement (LRL)	01	**langage naturel** ayant le statut (autre que celui de **langue officielle** ou de **langue de facto**) dans un **domaine juridictionnel** tel qu'énoncé dans une loi, un règlement ou tout autre instrument légal, qui accorde à une communauté de personnes (ou à ses **individus**) le droit d'utiliser ce **langage naturel** dans le contexte stipulé par l'(ou les) instrument(s) léga(ux) NOTE La langue reconnue légalement peut être spécifiée : (a) soit par l'identification d'une langue par son nom utilisé; ou, (b) soit par l'identification d'un peuple et ainsi de sa (ou ses) langue(s). EXEMPLE En plus des lois et règlements, les instruments légaux comprennent les ententes d'autonomie gouvernementale, les règlements en matière de revendication territoriale, les décisions de tribunal, la jurisprudence, etc.
3.075	ISO/IEC 15944-5:2008 (3.72)	legally recognized name (LRN)	99	**persona** associated with a **role** of a **Person** recognized as having legal status and so recognized in a **jurisdictional domain** as accepted or assigned in compliance with the rules applicable of that **jurisdictional domain**, i.e. as governing the **coded domain** of which the **LRN** is a member NOTE 1 A LRN may be of a general nature and thus be available for general use in commitment exchange or may arise from the application of a particular law, regulation, program or service of a jurisdictional domain and thus will have a specified use in commitment exchange. NOTE 2 The process of establishment of a LRN is usually accompanied by the assignment of a unique identifier. NOTE 3 A LRN is usually a registry entry in a register established by the jurisdictional domain (usually by a specified public administration within that jurisdictional domain) for the purpose of applying the applicable rules and registering and recording LRNs (and possible accompanying unique identifiers accordingly). NOTE 4 A Person may have more than one LRN (and associated LRN identifier).	nom légalement reconnu (NLR)	01	**persona** associée au **rôle** d'une **Personne** reconnue comme ayant un statut légal et ainsi reconnue dans un **domaine juridictionnel** comme acceptée ou attribuée conformément aux règles applicables de ce **domaine juridictionnel**, c.-à.-d. celles régissant le **domaine codé** dont le **NLR** est membre NOTE 1 Un NLR peut être de nature générale et ainsi être disponible pour usage général dans l'échange d'engagements ou peut découler de l'application d'une loi, d'un règlement, d'un programme ou d'un service particulier d'un domaine juridictionnel et ainsi avoir un usage spécifié dans l'échange d'engagements. NOTE 2 Ce processus d'établissement d'un NLR s'accompagne habituellement de l'attribution d'un identificateur unique. NOTE 3 Un NLR est habituellement une entrée de registre dans un registre établi par le domaine juridique (habituellement par une administration publique spécifiée dans ce domaine juridictionnel) aux fins d'application des règles applicables et de l'enregistrement et de l'inscription des NLR (et par conséquent de leurs identificateurs uniques possibles les accompagnants). NOTE 4 Une Personne peut avoir plus d'un NLR (et identificateur NLR connexe).

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.076	ISO/IEC 29187-1 (3.076)	LET Functional Services Support View (LET-FSV)	99	perspective of **learning transaction**s 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.	Vue du soutien des services d'AÉF (LET-FSV)	02	appréciation et évaluation sur les **transactions d'apprentissage**, limitée au fonctionnement informatique coopératif entre les systèmes d'information qui sont nécessaires à l'exécution des transactions d'EDI-ouvert NOTE Adapté de l'ISO/CEI 14662.
3.077	ISO/IEC 29187-2 (3.077)	LET- Operational View (LET-OV)	99	perspective of **learning transaction**s limited to those aspects regarding the making of learning decisions and **commitments** among **Persons**, which are needed for the description of a **learning transaction** NOTE Adapted from ISO/IEC 14662.	vue opérationnelle d'AÉF (LET-OV)	01	contenu des **transactions d'apprentissage** limitée aux facteurs déterminants les décisions d'apprentissage, et les **engagements** requis des **personnes** responsables de la description des **transactions d'apprentissage** NOTE Adapté de l'ISO/CEI 14662.
3.078	ISO/IEC 29187-1 (3.078)	LET privacy collaboration space (PCS)	99	modelling or inclusion of an **Open-edi scenario** of a **collaboration space** involving an **individual** as the **learner** in a potential or actualized **learning transaction** where the learner is an **individual** and therefore **privacy protection** requirements apply to **personal information** of that **individual** NOTE Adapted from ISO/IEC 15944-8.	espace collaboratif numérique de protection des données personnelles (PCS)	01	Modèle ou scenario reposant sur **un processus d'EDI-ouvert**, et créant un **espace collaboratif** impliquant tout **individu** apprenant , impliqué dans une **transaction d'apprentissage** ou l'apprenant est reconnu comme individu , et bénéficie donc des r**ègles de protection des données personnelles** applicables aux **renseignements personnelles** de cet **individu** NOTE Adapté de l'ISO/CEI 15944-8.
3.079	ISO/IEC 29187-1 (3.079)	LET provider	99	**Person**, as **organization** or **public administration** which provides a good, service, and/or right in the fields of learning, education or training as part of a **learning transaction**	fournisseur d'AÉF	01	**Personne**, à titre d'**organisation** ou d'a**dministration publique** qui fournit un bien, un service, et/ou un droit dans les domaines de l'apprentissage, de l'éducation ou de la formation comme partie d'une **transaction d'apprentissage**
3.080	ISO/IEC 2382-4:1999 (04.08.01)	list	99	ordered **set** of **data elements**	liste	02	**ensemble** d'**éléments de donnée** dont l'ordre est défini

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.081	ISO/IEC 15944-5:2008 (3.75)	localization	99	pertaining to or concerned with anything that is not global and is bound through specified sets of **constraints** of: (a) a linguistic nature including **natural** and **special languages** and associated multilingual requirements; (b) jurisdictional nature, i.e., legal, regulatory, geopolitical, etc.; (c) a sectoral nature, i.e., industry sector, scientific, professional, etc.; (d) a human rights nature, i.e., privacy, disabled/handicapped persons, etc.; (e) consumer behaviour requirements; and/or, (f) safety or health requirements. Within and among "locales", interoperability and harmonization objectives also apply	localisation	02	se rapportant à ou concernant tout ce qui n'est pas mondial et est lié par une série de **contraints** particuliers: (a) une nature linguistique comprenant les **langues naturelles** et **spéciales** ainsi que les exigences multilingues connexes; (b) une nature juridique, par exemple légale, de réglementation, géopolitique, etc.; (c) une nature sectorielle, par exemple, par exemple le secteur industriel, scientifique, professionnel, etc.; (d) une nature des droits de la personne, par exemple le respect de la vie privée, les handicapés, etc.; (e) les exigences en matière de comportement des consommateurs; et/ou; (f) les exigences en matière de sécurité et de santé. Des objectifs d'interopérabilité et d'harmonisation s'appliquent également à la localisation
3.082	ISO/IEC 15944-2:2006 (3.50)	**location**	99	place, either physical or electronic, that can be defined as an **address**	emplacement	01	lieu, physique ou électronique, pouvant être défini par une **adresse**
3.083	ISO/IEC 15944-1:2011 (3.34)	medium	99	physical material which serves as a functional unit, in or on which information or **data** is normally recorded, in which information or **data** can be retained and carried, from which information or **data** can be retrieved, and which is non-volatile in nature NOTE 1 This definition is independent of the material nature on which the information is recorded and/or technology used to record the information, (e.g., paper, photographic, (chemical), magnetic, optical, ICs (integrated circuits), as well as other categories no longer in common use such as vellum, parchment (and other animal skins), plastics, (e.g., bakelite or vinyl), textiles, (e.g., linen, canvas), metals, etc.). NOTE 2 The inclusion of the "non-volatile in nature" attribute is to cover latency and records retention requirements.	support	01	matériel physique qui sert d'unité fonctionnelle, et dans lequel ou sur lequel l'information ou les **données** sont normalement stockées, dans lequel de l'information ou des **données** peuvent être retenues et transportées, à partir duquel de l'information ou des **données** peuvent être extraites, et qui est non-volatile par nature NOTE 1 Cette définition est indépendante de la nature matérielle sur laquelle l'information est enregistrée et/ou de la technologie utilisée pour enregistrer l'information (par exemple du papier, des supports photographiques (chimiques), magnétiques, optiques, des circuits imprimés, ainsi que d'autres catégories qui ne sont plus utilisées de façon courante telles que le vélin, le parchemin (et autres peaux animales), les plastiques (par exemple la bakélite ou le vinyl), les textiles (par exemple le lin et la toile), les métaux, etc. NOTE 2 L'inclusion de l'attribut «nature non-volatile» couvre les exigences en matière de latence et de rétention des dossiers.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 3 This definition of "medium" is independent of: i) form or format of **recorded information**; ii) physical dimension and/or size; and, iii) any container or housing that is physically separate from material being housed and without which the medium can remain a functional unit. NOTE 4 This definition of "medium" also captures and integrates the following key properties: i) the property of medium as a material in or on which information or data can be recorded and retrieved; ii) the property of storage; iii) the property of physical carrier; iv) the property of physical manifestation, i.e., material; v) the property of a functional unit; and, vi) the property of (some degree of) stability of the material in or on which the information or data is recorded.			NOTE 3 La définition de «support» est indépendante des éléments suivants: i) la forme ou le format de l'information enregistrée; ii) la dimension physique et/ou la taille; et, iii) tout conteneur ou boîtier qui est séparé physiquement du matériel logé et sans lequel le support peut demeurer une unité fonctionnelle. NOTE 4 La définition de «support» reflète et intègre aussi les propriétés clés suivantes: i) propriété du support comme matériel dans ou sur lequel de l'information ou des données peuvent être stockées et extraites; ii) la propriété du stockage; iii) la propriété du porteur physique; iv) la propriété de la manifestation physique, par exemple le matériel; v) la propriété d'une unité fonctionnelle; et, vi) la propriété (jusqu'à un certain degré) de la stabilité du matériel dans ou sur lequel l'information ou les données sont stockées.
3.084	ISO 19115:2003 (4.9)	model	99	abstraction of some aspect of reality	modèle	01	abstraction de certains aspects de la réalité
3.085	ISO/IEC 15944-5:2008 (3.82)	multilingualism	99	ability to support not only **character sets** specific to a (natural) **language** (or family of **languages**) and associated **rules** but also **localization** requirements, i.e., use of a **language** from **jurisdictional domain**, sectoral and/or **consumer** marketplace perspectives	multilinguisme	01	capacité de supporter non seulement les **jeux de caractères** particuliers à une **langue naturelle** (ou une famille de **langues** ainsi que les **règles** connexes, mais aussi les exigences en matière de **localisation**, par ex. l'utilisation d'une **langue** dans une perspective de **domaine juridictionnel**, sectorielle et/ou de marché du **consommateur**
3.086	ISO/IEC 29187-1 (3.086)	mutually defined – recognized individual identity (md-rii) (in LET privacy protection)	99	**recognized individual identity (rii)** which is mutually defined and agreed to for use between the **LET provider** and the **individual**, as learner, in a **learning transaction** NOTE 1 The establishment of a mutually agreed to and recognized individual between a seller and individual, as buyer, does not extinguish the applicable privacy protection rights of that individual. NOTE 2 A mutually defined recognized individual identity (md-rii) shall be established between the seller and the individual no later than the end of the negotiation phase. NOTE 3 Use of a mutually defined recognized individual identity (md-rii) may not be permitted where external constraints apply. NOTE 4 Adapted from ISO/IEC 15944-8.	identité individuelle mutuellement définie reconnue (md-rii) (dans la protection de la vie privée concernant l'AÉF)	02	**identité individuelle reconnue** d'un commun accord pour usage entre le **fournisseur d'AÉF**, et l'**individu** comme apprenant, dans le cade d'une **transaction d'apprentissage** NOTE1 La mise en place d'un cadre reconnu d'un commun accord entre un opérateur et un apprenant, n'éteint pas les règles applicables à la protection des données personnelles de l'individu concerné. NOTE 2 Un cadre de définition de l'identité reconnu d'un commun accord doit être établi entre l'opérateur et l'apprenant, avant le terme de la période de négociation NOTE 3 L'utilisation d'un cadre de définition de l'identité reconnu d'un commun accord, ne pourra être conclu quand s'appliquent des règles et contraintes externes NOTE 4 Adapté de l'ISO/CEI 15944-8.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.087	ISO 5217: 2000 (1.1.2.13)	name	99	**designation** of an **object** by a linguistic expression	nom	01	**désignation** d'un **objet** par une unité linguistique
3.088	ISO 5217: 2000 (1.1.2.02)	natural language	99	**language** which is or was in active use in a community of people, and the **rules** of which are mainly deduced from the usage	langage naturel	01	**langage** qui est ou était pratiqué dans une communauté de personnes et **règles** qui sont essentiellement déduites de son usage
3.089	ISO 1087-1:2000 (3.1.1)	object	99	anything perceivable or conceivable NOTE Objects may be material, (e.g., engine, a sheet of paper, a diamond), or immaterial, (e.g., conversion ratio, a project play) or imagined, (e.g., a unicorn).	objet	01	tout ce qui peut être perçu ou conçu NOTE Les objets peuvent être matériels (par exemple un moteur, une feuille de papier, un diamant), immatériels (par exemple un rapport de conversion, un plan de projet) ou imaginaires (par exemple une licorne).
3.090	ISO/IEC 11179-1:2004 (3.3.22)	object class	99	set of ideas, abstractions, or things in the real world that can be identified with explicit boundaries and meaning and whose properties and behavior follow the same **rules**	classe d'objets	02	ensemble d'idées, d'abstractions ou de choses du monde réel qui peuvent être identifiées avec des limites et une signification explicites et dont les propriétés et le comportement suivent les mêmes **règles**
3.091	ISO/IEC 15944-5:2008 (3.87)	official language	99	**external constraint** in the form of a **natural language** specified by a **jurisdictional domain** for official use by **Persons** forming part of and/or subject to that j**urisdictional domain** for use in communication(s) either (1) within that **jurisdictional domain**; and/or, (2) among such **Persons**, where such communications are **recorded information** involving **commitment**(s) NOTE 1 Unless official language requirements state otherwise, Persons are free to choose their mutually acceptable natural language and/or special language for communications as well as exchange of commitments. NOTE 2 A jurisdictional domain decides whether or not it has an official language. If not, it will have a de facto language. NOTE 3 An official language(s) can be mandated for formal communications as well as provision of goods and services to Persons subject to that jurisdictional domain and for use in the legal and other conflict resolution system(s) of that jurisdictional domain, etc. NOTE 4 Where applicable, use of an official language may be required in the exercise of rights and obligations of individuals in that jurisdictional domain.	langue officielle	02	**contrainte externe** sous forme de **langage naturel** spécifié par un **domaine juridictionnel** pour usage officiel par des **Personnes** faisant partie ou sujettes de ce **domaine juridictionnel** dans la (ou les) communication(s) soit (1) à l'intérieur de ce **domaine juridictionnel**, soit (2) entre ces **Personnes**, lorsque ces communications sont une **information enregistrée** impliquant un (ou des) **engagement**(s) NOTE 1 Sauf exigence contraire concernant une langue officielle, les Personnes sont libres de choisir leur langage naturel mutuellement acceptable et/ou leur langue de spécialité dans les communications et l'échange d'engagements. NOTE 2 Un domaine juridictionnel décide s'il dispose d'une langue officielle. Dans le cas contraire, il disposera d'une langue de facto. NOTE 3 Une (ou des) langue(s) officielle(s) peut (ou peuvent) être exigée(s) dans les communications officielles et la disposition de biens et de services aux Personnes sujettes de ce domaine juridictionnel et dans le(s) système(s) juridique(s) et autre(s) système(s) de résolution de conflit de ce domaine juridictionnel, etc. NOTE 4 S'il y a lieu, l'utilisation d'une langue officielle peut être exigée dans l'exercice de droits et d'obligations des individus de ce domaine juridictionnel.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 5 Where an official language of a jurisdictional domain has a controlled vocabulary of the nature of a terminology, it may well have the characteristics of a special language. In such cases, the terminology to be used must be specified. NOTE 6 For an official language, the writing system(s) to be used shall be specified, where the spoken use of a natural language has more than one writing system. EXAMPLE 1 The spoken language of use of an official language may at times have more than one writing system. For example, three writing systems exist for the Inuktitut language. Canada uses two of these writing systems, namely, a Latin-1 based (Roman), the other is syllabic-based. The third is used in Russia and is Cyrillic based. EXAMPLE 2 Another example is that of Norway which has two official writing systems, both Latin-1 based, namely, Bokmål (Dano-Norwegian) and Nynorsk (New Norwegian). NOTE 7 A jurisdictional domain may have more than one official language but these may or may not have equal status. EXAMPLE Canada has two official languages; Switzerland has three, while the Union of South Africa has eleven official languages. NOTE 8 The BOV requirement of the use of a specified language will place that requirement on any FSV supporting service. EXAMPLE A BOV requirement of Arabic, Chinese, Russian, Japanese, Korean, etc., as an official language requires the FSV support service to be able to handle the associated character sets.			NOTE 5 Lorsqu'une langue officielle d'un domaine juridictionnel dispose d'un vocabulaire contrôlé de la nature d'une terminologie, elle peut très bien avoir les caractéristiques d'une langue de spécialité. Dans de tels cas, la terminologie à utiliser doit être spécifiée. NOTE 6 En ce qui concerne une langue officielle, le(s) système(s) d'écriture à utiliser doit(doit (doivent) être spécifié(s) lorsque l'usage parlé d'un langage naturel a plus d'un système d'écriture. EXEMPLE 1 La langue parlée d'une langue officielle peut parfois avoir plus d'un système d'écriture. L'Inuktitut, par ex., a trois systèmes d'écriture. Le Canada utilise deux de ces systèmes d'écriture, notamment l'alphabet latin-1 (romain) et l'alphabet syllabique. Le troisième est utilisé en Russie et est basé sur des caractères cyrilliques. EXEMPLE 2 Un autre exemple est celui de la Norvège qui a deux systèmes d'écriture officiels, tous les deux basés sur l'alphabet latin-1 : le Bokmål (Dano-Norvégien) et le Nynorsk (Nouveau Norvégien). NOTE 7 Un domaine juridictionnel peut avoir plusieurs langues officielles EXEMPLE le Canada a deux langues officielles, la Suisse trois et l'Afrique du Sud onze. NOTE 8 L'exigence BOV concernant l'usage d'une langue spécifique s'applique également à tout service de soutien FSV. EXEMPLE Une exigence BOV pour l'arabe, le chinois, le russe, le japonais, le coréen, etc. comme langue officielle exige que le service de soutien FSV soit capable de soutenir les jeux de caractères associés.
3.092	ISO/IEC 14662: 2010 (3.14)	Open-edi	99	**electronic data interchange** among multiple autonomous **Persons** to accomplish an explicitly shared **business** goal according to **Open-edi standards**	EDI-ouvert	01	**échange de données informatisé** par application des **normes d'EDI-ouvert** entre plusieurs **Personnes** autonomes visant un objectif d'**affaires** explicitement partagé
3.093	ISO/IEC 14662:2010 (3.16)	Open-edi Description Technique (OeDT)	99	specification method such as a **Formal Description Technique**, another methodology having the **characteristics** of a **Formal Description Technique**, or a combination of such techniques as needed to formally specify BOV concepts, in a computer processable form	Technique de description d'EDI-ouvert (OeDT)	02	méthode de spécification, **Technique de description formelle**, ou toute autre technique ayant les **caractéristiques** d'une **technique de description formelle**, ou combinaison de ces techniques, permettant de spécifier formellement les concepts de la BOV sous forme calculable par un ordinateur

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.094	ISO/IEC 15944-5:2008 (3.90)	Open-edi disposition	99	**process** governing the implementation of formally approved records retention, destruction (or expungement) or transfer of **recorded information** under the control of a **Person** which are documented in disposition authorities or similar instruments NOTE Adapted from ISO 15489-1.	disposition d'EDI-ouvert	02	**processus** gouvernant l'application d'une rétention d'enregistrement formellement approuvée, la destruction (ou radiation) ou le transfert d'**information enregistrée** sous le contrôle d'une **Personne** qui sont documentés dans des autorités de disposition ou instruments semblables NOTE Adapté de l'ISO 15489-1.
3.095	ISO/IEC 14662: 2010 (3.17)	Open-edi Party (OeP)	99	**Person** that participates in **Open-edi** NOTE Often referred to generically in this, and other eBusiness standards, (e.g., parts of the ISO/IEC 15944 multipart "eBusiness" standard) as "party" or "parties" for any entity modelled as a Person as playing a role in Open-edi scenarios.	partenaire d'EDI-ouvert (OeP)	01	**Personne** participant à l'**EDI-ouvert** NOTE Souvent mentionnée de façon générique dans la présente norme, et dans d'autres normes d'eAffaires (par ex. dans certaines parties de la norme multiparties d' « eAffaires » ISO/CEI 15944), comme « partie » ou « parties » pour toute entité modélisée comme une Personne jouant un rôle dans les scénarios d'EDI-ouvert.
3.096	ISO/IEC 29187-1 (3.096)	Open-edi Record Retention (OeRR) (in LET privacy protection)	99	specification of a period of time that a **set of recorded information** must be kept by a **Person** in order to meet operational, legal, regulatory, fiscal or other requirements as specified in the **external constraints** (or **internal constraints**) applicable to a **Person** who is a party to a **learning transaction** NOTE Adapted from ISO/IEC 15944-5.	rétention d'enregistrement d'EDI-ouvert (OeRR) (dans la protection de la vie privée concernant l'AÉF)	02	spécification d'une période de temps pendant laquelle un **ensemble d'informations enregistrées** doit être conserve par une **Personne** afin de répondre à des exigences opérationnelles, légales, de réglementation, fiscales ou autres, tel que spécifié dans les **contraintes externes** (ou les **contraintes internes**) applicables à une **Personne** faisant partie d'une **transaction d'apprentissage** NOTE Adapté de l'ISO/CEI 15944-5.
3.097	ISO/IEC 14662:2010 (3.22)	Open-edi system	99	**information technology system (IT system)** which enables an **Open-edi Party** to participate in Open-edi transactions	système d'EDI-ouvert	01	**système d'information (IT system)** permettant à un partenaire d'**EDI-ouvert** de prendre part à des transactions d'EDI-ouvert
3.098	ISO/IEC 6523-1:1998 (3.1)	organization	99	unique framework of authority within which a Person or persons act, or are designated to act, towards some purpose NOTE The kinds of organizations covered by this International Standard include the following examples: EXAMPLE 1 An organization incorporated under law. EXAMPLE 2 An unincorporated organization or activity providing goods and/or services including: 1) partnerships; 2) social or other non-profit organizations or similar bodies in which ownership or control is vested in a group of individuals; 3) sole proprietorships 4) governmental bodies.	organisation	02	cadre unique d'autorité dans lequel une ou plusieurs personnes agissent ou sont désignées pour agir afin d'atteindre un certain but NOTE Les types d'organisations couverts par la présente partie de l'ISO/CEI 6523 comprennent par exemple les éléments suivants: EXEMPLE 1 Organisations constituées suivant des formes juridiques prévues par la loi. EXEMPLE 2 Autres organisations ou activités fournissant des biens et/ou des services, tels que: 1) sociétés en participation; 2) organismes sociaux ou autres à but non lucratif dans lesquels le droit de propriété ou le contrôle est dévolu à un groupe de personnes; 3) entreprises individuelles; 4) administrations et organismes de l'état.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				EXAMPLE 3 Groupings of the above types of organizations where there is a need to identify these in information interchange.			EXEMPLE 3 Regroupements des organisations des types ci-dessus, lorsqu'il est nécessaire de les identifier pour l'échange d'informations.
3.099	ISO/IEC 6523-1:1998 (3.2)	organization part	99	any department, service or other **entity** within an **organization**, which needs to be identified for information interchange	partie d'organisation	02	n'importe quel département, service ou autre **entité** au sein d'une **organisation**, qu'il est nécessaire d'identifier pour l'échange d'informations
3.100	ISO/IEC 15944-1:2011 (3.46)	organization Person	99	**organization part** which has the properties of a **Person** and thus is able to make **commitments** on behalf of that **organization** NOTE 1 An organization can have one or more organization Persons. NOTE 2 An organization Person is deemed to represent and act on behalf of the organization and to do so in a specified capacity. NOTE 3 An organization Person can be a "natural Person" such as an employee or officer of the organization. NOTE 4 An organization Person can be a legal Person, i.e., another organization.	Personne d'organisation	02	**partie d'une organisation** qui a les propriétés d'une **Personne** et est ainsi capable de prendre des **engagements** au nom de cette **organisation** NOTE 1 Une organisation peut avoir une ou plusieurs Personnes d'organisation. NOTE 2 Une Personne d'organisation est considérée représenter une organisation et agir en son nom, et ce à titre de capacité spécifiée. NOTE 3 Une Personne d'organisation peut être une «personne physique» telle qu'un employé ou un agent de l'organisation. NOTE 4 Une Personne d'organisation peut être une personne morale, c.-à-d. une autre organisation.
3.101	ISO/IEC 14662: 2010 (3.24)	Person	99	**entity**, i.e., a natural or legal Person, recognized by law as having legal rights and duties, able to make **commitment**(s), assume and fulfill resulting obligation(s), and able of being held accountable for its action(s) NOTE 1 Synonyms for "legal Person" include "artificial Person", "body corporate", etc., depending on the terminology used in competent jurisdictions. NOTE 2 "Person" is capitalized to indicate that it is being used as formally defined in the standards and to differentiate it from its day-to-day use. NOTE 3 Minimum and common external constraints applicable to a learning transaction often require one to differentiate among three common subtypes of Person, namely "individual", "organization", and "public administration".	Personne	02	**entité**, c.-à-d. une personne physique ou morale, reconnue par la loi comme ayant des droits et des devoirs, capable de prendre des **engagements**, d'assumer et de remplir les obligations résultantes, et capable d'être tenue responsable de ses actions NOTE 1 Parmi les synonymes de «personne morale», on trouve «personne juridique», «personne fictive», «corporation», etc., selon la terminologie utilisée par les juridictions compétentes. NOTE 2 « Personne » prend la majuscule pour indiquer que ce terme est utilisé tel que défini officiellement dans les normes et pur le différencier de son usage ordinaire. NOTE 3 Les exigences minima et communes applicables aux transactions d'affaires obligent souvent à faire une différence entre les trois sous-catégories communes de « Personne », notamment « individu », « organisation », « administration publique».
3.102	ISO/IEC 29187-1 (3.102)	persona	99	set of **data elements** and their values by which a **Person** wishes to be known and thus identified in a **learning transaction** Note Adapted from ISO/IEC 15944-1	persona	02	série d'**éléments de données** et leurs valeurs selon lesquelles une **Personne** désire être connue et ainsi identifiée dans une **transaction d'apprentissage** NOTE Adapté de l'ISO/ICEI 15944-1.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.103	ISO/IEC 15944-5:2008 (3.103)	personal information	99	any information about an identifiable **individual** that is recorded in any form, including electronically or on paper NOTE Some examples would be record information about a person's religion, age, financial transactions, medical history, address, or blood type.	renseignements personnels	01	tout renseignement au sujet d'un **individu** identifiable, qui est enregistré sous une forme quelconque, y compris électroniquement ou sur papier NOTE Cela comprend, par exemple, les informations enregistrées à propos de la religion, de l'âge, des opérations financières, du passé médical, de l'adresse ou du groupe sanguin de quelqu'un.
3.104	ISO/IEC 15944-1:2011 (3.52)	persona Registration Schema (pRS)	99	formal **definition** of the **data** fields contained in the specification of a **persona** of a **Person** and the allowable contents of those fields, including the **rules** for the assignment of **identifiers**. (This may also be referred to as a "**persona** profile" of a **Person**)	schéma d'enregistrement d'une persona (pRS)	01	**définition** officielle des champs de **données** contenus dans la description d'une **persona** d'une **Personne**, et du contenu autorisé de ces champs, y-compris les **règles** d'attribution des **identificateurs**. (Cette notion peut également être désignée comme le profil **persona** d'une **Personne**)
3.105	ISO/IEC 29187-1 (3.105)	Person authentication	99	provision of the assurance of a **recognized Person identity (rPi)** (sufficient for the purpose of the **learning transaction**) by corroboration NOTE Adapted from ISO/IEC 15944-1.	authentification d'une Personne	02	don de l'assurance de l'**identité d'une Personne reconnue (rPi)** (suffisante aux fins de la **transaction d'apprentissage** par corroboration NOTE Adapté de l'ISO/CEI 15944-1.
3.106	ISO/IEC 29187-1 (3.106)	Person identity (Pi) (in LET privacy protection)	99	combination of **persona information** and **identifier** used by a **Person** in a **learning transaction** NOTE Adapted from ISO/IEC 15944-1	identité d'une Personne (Pi) (dans la protection de la vie privée concernant l'AÉF)	02	combinaison de l'**information** d'une **persona** et de l'**identificateur** utilisé par une **Personne** dans une **transaction d'apprentissage** NOTE Adapté de l'ISO/ICEI 15944-1.
3.107	ISO/IEC 15944-1:2011 (3.50)	Person signature	99	signature, i.e., a **name** representation, distinguishing mark or usual mark, which is created by and pertains to a **Person**	signature d'une Personne	02	signature, c.-à-d.la représentation d'un **nom**, marque de distinction ou marque habituelle, qui est créée par une **Personne** et se rapporte à celle-ci
3.108	ISO/IEC 15944-8 (3.102)	personal information filing system	99	any structured set of **personal information** which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis	système de classement des renseignements personnels	01	tout ensemble structuré de **renseignements personnels** accessible en fonction de critères spécifiques, que l'accès soit centralisé, décentralisé ou dispersé, sur une base fonctionnelle ou géographique
3.109	ISO/IEC 15944-2:2006 (3.80)	physical address	99	**address** that is used/recognized by a postal authority and/or courier service to deliver information item(s), material object(s), or **business object(s)** to a contact at either an actual **address** or a pick-up point **address**, (e.g., P.O. Box, rural route, etc.)	adresse physique	02	**adresse** qui est utilisée/reconnue par une autorité postale et/ou un service de messagerie pour livraison d'article(s) d'information, d'**objet(s)** matériel(s), ou d'**objet(s)** d'**affaires** à un contact, soit à une **adresse** réelle, soit à une **adresse** de point de ramassage, (par ex. une boîte postale, une route rurale, etc.)

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.110	ISO/IEC 15944-5:2008 (3.104)	pivot code set	99	set of **ID codes** in a **coded domain** which is made publicly known and available, the most stable, representing the defined semantics. (Most often it is the same as the **ID code**) NOTE 1 The use of the pivot code set (as per Part 5) as distinguished from the ID code supports the requirement of a Source Authority to maintain internally and on a confidential basis the ID code of its members. NOTE 2 At times a coded domain has more than one valid code set, (e.g., ISO 639, ISO 3166, etc.) EXAMPLE In ISO 3166-1 the 3-digit numeric code is the pivot. The 2-alpha and 3-alpha code sets can change when the name of the entity referenced is changed by that entity.	ensemble de codes pivots	01	ensemble de **codes ID** dans un **domaine codé** qui est rendu public et disponible, le plus stable représentant la sémantique définie. (Le plus souvent, c'est le même que le **code ID**) NOTE 1 L'utilisation de l'ensemble de codes pivots différent du code ID appuie les exigences d'une Autorité de source pour conserver à l'interne et confidentiellement le code ID de ses membres. NOTE 2 Parfois, un domaine codé a plus d'un ensemble de codes valides (par ex. l'ISO 639, l'ISO 3166, etc.) EXEMPLE Dans l'ISO 3166-1, le code numérique à 3 chiffres est le code pivot. L'ensemble des codes alphabétique à 2 lettres et alphabétique à 3 lettres peut changer lorsque le nom de l'entité référencée est changé par cette entité.
3.111	ISO/IEC 15944-5:2008 (3.105)	pivot ID code	99	most stable **ID code** assigned to identify a member of a **coded domain** where more than one **ID code** may be assigned and/or associated with a member of that **coded domain** EXAMPLE ISO 3166-1:1997 (E/F) "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes/Codes pour la représentations des norms de pays et de leur subdivisions - Partie 1: Codes pays" contains three code sets: (a) a three digit numeric code;; (b) a two alpha code; (c) a three alpha code. In this case, the three digit numeric code serves as the pivot code. It is the most stable, remains the same even though the two alpha and/or three alpha codes may and do change.	code ID pivot	01	**code ID** le plus stable attribué pour identifier un membre d'un **domaine codé** lorsque plusieurs **codes ID** peuvent être attribués et/ou rattachés à un membre de ce **domaine codé** EXEMPLE L'ISO 3166-1 :1997 (E/F) « Codes for the representation of names of countries and their subdivisions - Part 1: Country codes/Codes pour la représentation des noms de pays et de leur subdivisions - Partie 1: Codes pays » contient trois ensembles de codes : (a) un code numérique à trois chiffres; (b) un code alphabétique à deux lettres; et, (c) un code alphabétique à trois lettres. Dans ce cas, le code numérique à trois chiffres sert de code pivot. C'est le plus stable, il reste le même, même si les codes alphabétiques à deux et trois lettres peuvent changer (comme cela se produit).
3.112	ISO/IEC 15944-2:2006 (3.81)	principle	99	fundamental, primary assumption and quality which constitutes a source of action determining particular objectives or results NOTE 1 A principle is usually enforced by rules that affect its boundaries. NOTE 2 A principle is usually supported through one or more rules. NOTE 3 A principle is usually part of a set of principles which together form a unified whole. EXAMPLE Within a jurisdictional domain, examples of a set of principles include a charter, a constitution, etc.	principe	01	hypothèse fondamentale et primaire, et qualité qui constitue une source d'action pour déterminer des objectifs ou des résultats particuliers NOTE 1 Un principe est habituellement mis en vigueur par des règles qui touchent ses limites. NOTE 2 Un principe est habituellement soutenu par une ou plusieurs règles. NOTE 3 Un principe fait habituellement partie d'un ensemble de principes qui ensemble forment un tout unifié. EXEMPLE Dans un domaine juridique, une charte, une constitution, etc., sont des exemples d'un ensemble de principes.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.113	ISO/IEC 29187-1 (3.113)	privacy protection (in LET privacy protection)	99	set of **external constraints** of a **jurisdictional domain** pertaining to **recorded information** on or about an identifiable **individua**l, i.e., **personal information**, with respect to the creation, collection, management, retention, access and use and/or distribution of such **recorded information** about that **individual** including its accuracy, timeliness, and relevancy NOTE 1 Recorded information collected or created for a specific purpose on an identifiable individual, i.e., the explicitly shared goal of the learning transaction involving an individual shall not be used for another purpose without the explicit and informed consent of the individual to whom the recorded information pertains. NOTE 2 Privacy requirements include the right of an individual to be able to view the recorded information about him/her and to request corrections to the same in order to ensure that such recorded information is accurate and up-to-date. NOTE 3 Where jurisdictional domains have legal requirements which override privacy protection requirements these must be specified, (e.g., national security, investigations by law enforcement agencies, etc.). NOTE 4 Adapted from ISO/IEC 15944-8.	protection de la vie privée (dans la protection de la vie privée concernant l'AÉF)	02	ensemble de **contraintes externes** exercées sur un **domaine juridictionnel** relatives à l'**information enregistrée** ou à propos d'un **individu** identifiable, c.-à.-d. des **renseignements personnels**, en ce qui concerne la création, la collecte, la gestion, la rétention, l'accès et l'utilisation et/ou la distribution d'une telle i**nformation enregistrée** relative à cet **individu**, y compris son exactitude, son opportunité et sa pertinence NOTE 1 L'information enregistrée recueillie ou créée dans un but spécifique concernant un individu identifiable (c.-à.-d. le but partagé et explicite de la transaction d'apprentissage concernant un individu) ne peut être utilisée dans un autre but sans le consentement explicite et informé de l'individu auquel l'information enregistrée se rapporte. NOTE 2 Les exigences en matière de vie privée incluent le droit d'un individu de pouvoir examiner l'information enregistrée le (ou la) concernant, et de demander d'y apporter des corrections afin de s'assurer que l'information enregistrée est exacte et à jour. NOTE 3 Lorsque des domaines juridictionnels ont des exigences légales qui ont préséance sur les exigences en matière de protection de la vie privée (par ex. la sécurité nationale, les enquêtes policières, etc.), ils doivent être spécifiés. NOTE 4 Adapté de l'ISO/CEI 15944-8.
3.114	ISO/IEC 29187-1 (3.114)	privacy protection officer (PPO) (in LET privacy protection)	99	**organization Person** authorized by the **organization** to act on behalf of that **organization** and entrusted by the organization as the officer responsible for the overall governance and implementation of the privacy protection requirements for information life cycle management not only within that **organization** but also with respect to any **electronic data interchange** of **personal information** on the **individual** concerned with parties to the **learning transaction**, including a **regulator** where required, as well as any **agents**, **third parties** involved in that **learning transaction** NOTE Adapted from ISO/IEC 15944-8.	officier responsable de la protection des données personnelles (PPO) (dans la protection de la vie privée concernant l'AÉF)	01	**Personne d'organisation** autorisée par l'**organisation** à agir au nom de cette **organisation** et mandatée par l'**organisation** comme officier responsable de la gouvernance et de l'application des exigences de protection de la vie privée pour la gestion du cycle de vie de l'information à l'intérieur de l'**organisation** et dans les opérations d'**échanges de données informatisés** contenant des **informations personnelles** sur un **individu** concerné par les tiers d'une t**ransaction d'apprentissage** incluant une **autorité de réglementation** selon le besoin, ainsi que tous **agents** ou **tiers** impliqués dans une **transaction d'apprentissage** NOTE Adapté de l'ISO/CEI 15944-8.
3.115	ISO/IEC 15944-1:2011 (3.53)	process	99	series of actions or events taking place in a defined manner leading to the accomplishment of an expected result	processus	01	série d'actions ou d'événements qui se produisent d'une manière définie et qui aboutissent à un résultat attendu

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.116	ISO/IEC 15944-8:2010-06-23 (3.111)	processing of personal information	99	any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction	traitement de renseignements personels	01	toute opération ou groupe d'opérations réalisé par traitement de données personnelles, par des moyens automatiques ou non, tels que la collecte, l'organisation, le stockage, l'altération, la recherche, la consultation, l'usage, la transmission, la dissémination ou tout autre pratique rendant disponible , alignant ou combinant, bloquant ou détruisant les dites informations personnelles
3.117	ISO/IEC 11179-1:2004 (3.3.29)	property	99	peculiarity common to all members of an **object class**	propriété	02	particularité commune à tous les membres d'une **classe d'objets**
3.118	ISO/IEC 29187-1 3.118	pseudonym	99	use of a **persona** or other **identifier** by an **individual** which is different from that used by the **individual** with the intention that it be not linkable to that individual NOTE Adapted from ISO TS 25237.	pseudonyme	01	utilisation d'une **persona** ou d'un autre **identificateur** par un **individu** qui est différèrent de celle qui est utilisée par l'**individu** dans l'intention de ne pas pouvoir établir de lien avec cet individu NOTE Adapté de l'ISO TS 25237.
3.119	ISO/IEC 15944-8 (3.114)	pseudonymization	99	particular type of anonymization that removes the associate with an **individual** and adds an associate between a particular set of **characteristics** relating to the **individual** and one more **pseudonym** NOTE Adapted from ISO TS 25237.	pseudonymisation	02	type particulier d'anonymisation qui supprime le correspondant avec un **individu** et ajoute un correspondant entre un ensemble particulier de **caractéristiques** se rapportant à cet **individu** et un autre **pseudonyme** NOTE Adapté d'ISO TS 25237.
3.120	ISO/IEC 15944-1:2011 (3.54)	public administration	99	**entity**, i.e., a **Person**, which is an **organization** and has the added **attribute** of being authorized to act on behalf of a **regulator**	administration publique	02	**entité,** ou **Personne**, qui est une **organisation** et a l'**attribut** supplémentaire d'être autorisé à agir au nom d'une **autorité de réglementation**
3.121	ISO/IEC 15944-5:2008 (3.113)	public policy	99	category of **external constraints** of a **jurisdictional domain** specified in the form of a right of an **individual** or a requirement of an **organization** and/or **public administration** with respect to an **individual** pertaining to any exchange of **commitments** among the parties concerned involving a good, service and/or right including information management and interchange requirements	politique publique	02	catégorie de **contraintes externes** d'un **domaine juridictionnel** spécifié sous la forme d'un droit d'un **individu** ou d'une exigence exercée sur une **organisation** et/ou une **administration publique** en ce qui concerne un **individu** relatif à tout échange d'**engagements** entre les parties concernées à propos d'un bien, d'un service et/ou d'un droit, y compris les exigences en matière de gestion de l'information et d'échange

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 1 Public policy requirements may apply to any one, all or combinations of the fundamental activities comprising a learning transaction, i.e., planning, identification, negotiation, actualization and post-actualization. {See further Clause 6.3 "Rules governing the process component" in ISO/IEC 15944-1:2002} NOTE 2 It is up to each jurisdictional domain to determine whether or not the age of an individual qualifies a public policy requirement, (e.g., those which specifically apply to an individual under the age of thirteen (13) as a "child", those which require an individual to have attained the age of adulthood, (e.g., 18 years or 21 years of age) of an individual to be able to make commitments of a certain nature. NOTE 3 Jurisdictional domains may have consumer protection or privacy requirements which apply specifically to individuals who are considered to be "children", "minors", etc. (e.g. those who have not reached their 18th or 21st birthday according to the rules of the applicable jurisdictional domain).			NOTE 1 Des exigences en matière de politique publique peuvent s'appliquer à l'une ou à toutes les combinaisons des activités fondamentales touchant une transaction d'apprentissage, c.-à.-d. la planification, l'identification, la négociation, l'actualisation et la post-actualisation. {Voir plus loin la Clause 6.3 « Règles régissant la composante de processus » dans l'ISO/IEC 15944-1:2002} NOTE 2 Il appartient à chaque domaine juridictionnel de déterminer si l'âge d'un individu qualifie une exigence en matière de politique publique (par ex. celles qui s'appliquent spécifiquement à un individu de moins de treize (13) ans en tant qu'« enfant », celles qui exigent qu'un individu ait atteint l'âge adulte, (par ex. 18 ou 21 ans), pour qu'un individu soit en mesure de prendre un engagement d'une certaine nature. NOTE 3 Des domaines juridictionnels peuvent avoir des exigences en matière de protection du consommateur ou de la vie privée qui s'appliquent spécifiquement à des individus qui sont considérés comme des « enfants » ou des « mineurs », etc. (c.-à.-d. ceux qui n'ont pas encore atteint leur 18 è ou 21è anniversaire de naissance conformément aux règles du domaine juridictionnel applicable).
3.122	ISO/IEC 15944-8 (3.118)	publicly available personal information	99	**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 EXAMPE 1 Examples of 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 Examples of 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.	renseignements personels d'accès public	01	**renseignements personnelle** sur un **individu**, que celui-ci produit délibérément ou autorise de rendre accessible, ou qui est obtenue légalement par accès à: (a) les bases de données gouvernementales accessibles au public; ou, (b) les informations que la loi prévoit de rendre publiques EXEMPLE 1 Les informations personnelles qu'un individu fournit ou dont il autorise délibérément la diffusion, incluant ainsi les registres publics du téléphone, les publicités dans la presse, les matériaux publiés, les éléments postés sur internet ayant cette nature, etc. EX EMPLE 2 Les informations contenues dans les bases de données gouvernementales publiquement accessibles incluant les listes électorales, les transactions sur les propriétés, ou toute autre information personnelle étant publiquement requise pour les besoins de la justice

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.123	ISO/IEC 29187-1 (3.123)	recognized individual identity (rii) (in LET privacy protection)	99	identity of an **individual**, i.e., **individual identity**, established to the extent necessary for the specific purpose of a **learning transaction** NOTE Adapted from ISO/IEC 15944-8.	identité individuelle reconnue (rii) (dans la protection de la vie privée concernant l'AÉF)	02	**identité d'un individu,** c'-a.-d., identité **individuelle**, établie avec la portée nécessaire au besoin spécifique d'une **transaction d'apprentissage** NOTE Adapté de l'ISO/CEI 15944-8.
3.124	ISO/IEC 15944-5:2008 (3.114)	recognized individual name (RIN)	99	**persona** of an **individual** having the properties of a **legally recognized name (LRN)** NOTE 1 On the whole, a persona presented by an individual should have a basis in law (or recognized jurisdictional domain) in order to be considered as the basis for a recognized individual name (RIN). NOTE 2 An individual may have more than one RIN and more than one RIN at the same time. NOTE 3 The establishment of a RIN is usually accompanied by the assignment of a unique identifier, i.e. by the jurisdictional domain (or public administration) which recognizes the persona as a RIN.	nom reconnu d'individu (RIN)	01	**persona** d'un **individu** ayant les propriétés d'un non **reconnu légalement (LRN)** NOTE 1 En définitive, une persona présentée par un individu doit avoir une base légale (ou un domaine juridictionnel reconnu) pour être considérée comme base d'un nom reconnu d'individu (NRI). NOTE 2 Un individu peut avoir plus d'un NRI ou plus d'un nom reconnu d'individu en même temps. NOTE 3 L'établissement d'un nom individuel reconnu s'accompagne généralement de l'attribution d'un identificateur unique par le domaine juridictionnel (ou l'administration publique) qui reconnaît la persona comme nom reconnu d'individu (NRI).
3.125	ISO/IEC 29187-1 (3.125)	recognized Person identity (rPi) (in LET privacy protection)	99	identity of a **Person**, i.e., **Person identity**, established to the extent necessary for a specific purpose in a **learning transaction** NOTE Adapted from ISO/IEC 15944-1.	identité d'une Personne reconnue (rPi) (dans la protection de la vie privée concernant l'AÉF)	02	**identité d'une Personne** établie selon les besoins nécessaires d'une **transaction d'apprentissage** dans un but spécifique NOTE Adapté de l'ISO/CEI 15944-1.
3.126	ISO/IEC 15944-1:2011 (3.56)	recorded information	99	any **information** that is recorded on or in a **medium** irrespective of form, recording **medium** or technology used, and in a manner allowing for storage and retrieval NOTE 1 This is a generic definition and is independent of any ontology, (e.g., those of "facts" versus "data" versus "information" versus "intelligence" versus "knowledge", etc.). NOTE 2 Through the use of the term "information," all attributes of this term are inherited in this definition.	information enregistrée	02	toute **information** enregistrée sur ou dans un **support** quelle que soit sa forme, le **support** de stockage ou la technologie utilisés, et de façon à permettre son stockage et son extraction NOTE 1 Cette définition est générique et indépendante de toute ontologie, (par exemple le point de vue des «faits» par rapport aux «données», à «l'information», aux «renseignements», à la «connaissance», etc.). NOTE 2 Dans l'utilisation du terme «information», tous les attributs de ce terme sont hérités dans cette définition.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 3 This definition covers: (i) any form of **recorded information**, means of recording, and any medium on which information can be recorded; and, (ii) all types of **recorded information** including all data types, instructions or software, databases, etc.			NOTE 3 Cette définition couvre les éléments suivants : (i) toute forme d'information enregistrée, tout moyen d'enregistrement, et tout support sur lequel l'information peut être enregistrée; et, (ii) tous types d'information enregistrée, y compris tous les types de données, instructions ou logiciels, bases de données, etc.
3.127	ISO 19135: 2005 (4.1.9)	register	99	set of files containing **identifiers** assigned to items with descriptions of the associated items	registre	01	ensemble de fichiers contenant des **identificateurs** attribués à des articles avec une description des articles qui s'y rattachent
3.128	ISO/IEC 15944-2:2006 (3.95)	registration	99	**rule**-based **process**, explicitly stated, involving the use of one or more **data elements**, whose value (or combination of values) are used to identify uniquely the results of assigning an OeRI	enregistrement	01	**processus** à **base** de règles, énoncé explicitement, impliquant l'utilisation d'un ou de plusieurs **éléments de données**, dont la valeur (ou la combinaison de valeurs) sert à identifier uniquement les résultats de l'attribution d'un OeRI
3.129	ISO/IEC 15944-1:2011 (3.57)	Registration Authority (RA)	99	**Person** responsible for the maintenance of one or more **Registration Schemas (RS)** including the assignment of a unique **identifier** for each recognized **entity** in a **Registration Schema (RS)**	Autorité d'enregistrement (RA)	02	**Personne** responsable du maintien d'un ou de plusieurs **schémas d'enregistrement (RS)**, y compris l'attribution d'un **identificateur** unique pour chaque **entité** reconnue d'un **schéma d'enregistrement (RS)**
3.130	ISO/IEC 11179-1:2004 (3.3.32)	Registration Authority Identifier (RAI)	99	**identifier** assigned to a **Registration Authority (RA)**	identificateur d'Autorité d'enregis-trement (RAI)	01	**identificateur** attribué à une **autorité d'enregistrement (RA)**
3.131	ISO/IEC 15944-1:2011 (3.58)	Registration Schema (RS)	99	formal **definition** of a set of **rules** governing the **data** fields for the description of an **entity** and the allowable contents of those fields, including the **rules** for the assignment of **identifiers**	Schéma d'enregistrement (RS)	01	**définition** officielle d'un ensemble de **règles** régissant les champs de **données** pour la description d'une **entité** ainsi que le contenu autorisé de ces champs, y-compris les **règles** d'attribution des **identificateurs**
3.132	ISO/IEC 29187-1 (3.132)	Registration Schema (based) – recognized individual identity (RS-rii) (in LET privacy protection)	99	**recognized individual identity (rii)** for use in a **learning transaction**, by the buyer as an **individual**, which is one based on the use by an **individual** as a member of a specified **Registration Schema (RS)** of a particular **Registration Authority (RA)** NOTE Adapted from ISO/IEC 15944-8.	identité individuelle reconnue basée sur un schéma d'enregistrement (RS-rii) (dans la protection de la vie privée concernant l'AÉF)	02	**identité individuelle reconnue (rii)** à utiliser dans une **transaction d'apprentissage** par un acheteur à titre d'**individu**, qui est basée sur l'utilisation par un **individu** en tant que membre d'un **schéma d'enregistrement (RS)** spécifié d'une **autorité d'enregistrement (RA)** particulière NOTE Adapté de l'ISO/CEI 159944-8.
3.133	ISO/IEC 15944-2:2006 (3.99)	registry	99	information system on which a **register** is maintained	registre	01	système d'information sur lequel est maintenu un **registre**

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.134	ISO/IEC 29187-1 (3.134)	regulator	99	**Person** who has authority to prescribe **external constraints** which serve as **principles**, policies or **rules** governing or prescribing the behaviour of **Persons** involved in a **learning transaction** as well as the provisioning of goods, services, and/or rights interchanged NOTE Adapted from ISO/IEC 15944-1.	autorité de réglementation	02	**Personne** autorisée à prescrire des **contraintes externes** qui servent de **principes**, de politiques ou de **règles** régissant ou prescrivant le comportement des **Personnes** concernées par une **transaction d'apprentissage**, ainsi que la fourniture des biens, services et/ou droits échangés NOTE Adapté de l'ISO/CEI 15944-1.
3.135	ISO/IEC 29187-1 (3.135)	regulatory learning transaction (RLT)	99	class of **learning transaction**s for which the explicitly shared goal has been established and specified by a **jurisdictional domain**, as a **Person** in the **role** of a **regulator** NOTE 1 A regulatory learning transaction (RLT) can itself be modelled as a stand-alone learning transaction and associated scenario(s). For example, the filing of a tax return, the making of a customs declaration, the request for and issuance of a license, the provision of a specified service of a public administration, a mandatory filing of any kind with a regulator, etc. NOTE 2 A regulatory learning transaction (modelled as a scenario) can form part of another learning transaction. NOTE 3 A RLT may apply to a LET provider only, a learner only or both, as well as any combination of parties to a learning transaction. NOTE 4 A RLT may require or prohibit the use of an agent or third party. NOTE 5 A regulatory learning transaction (RLT) may be specific to the nature of the good, services and/or right forming part of a learning transaction. NOTE 6 Adapted from ISO/IEC 15944-5.	transaction d'apprentissage réglementaire (RLT)	02	classe de **transaction d'apprentissage** pour laquelle l'objectif partagé explicitement a été établi et spécifié par un **domaine juridictionnel**, à titre de **Personne** dans le **rôle** d'une **autorité de réglementation** NOTE 1 Une transaction d'apprentissage réglementaire (RBT) peut elle-même être modélisée comme transaction d'apprentissage autonome, et comme scénarios connexes. Par exemple, une déclaration de revenu, une déclaration de douane, une demande de délivrance de permis, une disposition d'un service spécifique d'une administration publique, une déclaration obligatoire de toute nature auprès d'une autorité de réglementation, etc. NOTE 2 Une transaction d'apprentissage réglementaire (modélisée comme scénario) peut faire partie d'une autre transaction d'apprentissage NOTE 3 Une transaction d'apprentissage réglementaire peut ne s'appliquer qu'à un vendeur, un acheteur, ou au deux, ainsi qu'à n'importe quelle combinaison de parties dans une transaction d'apprentissage. NOTE 4 Une transaction d'apprentissage réglementaire (RLT) peut exiger ou prohiber l'utilisation d'un agent ou d'un tiers de confiance. NOTE 5 Une transaction d'apprentissage règlementée (RLT) peut être spécifique à la nature du bien, des services et/ou du droit faisant partie d'une transaction d'apprentissage. NOTE 6 Adapté de l'ISO/CEI 15944-5.
3.136	ISO/IEC 2382-12:1988 (12.04.01)	retention period	99	length of time for which **data** on a **data medium** is to be preserved	période de rétention	02	durée pendant laquelle des **données** enregistrées sur un **support de données** doivent être conservées
3.137	ISO/IEC 14662: 2010 (3.25)	role	99	specification which models an external intended behaviour (as allowed within a **scenario**) of an **Open-edi Party**	rôle	01	spécification qui modélise le comportement externe attendu d'un partenaire d'**EDI-ouvert** dans le cadre permis par un **scénario**

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.138	ISO/IEC 15944-2:2006 (3.101)	rule	99	statement governing conduct, procedure, conditions and relations NOTE 1 Rules specify conditions that must be complied with. These may include relations among objects and their attributes. NOTE 2 Rules are of a mandatory or conditional nature. NOTE 3 In Open-edi, rules formally specify the commitment(s) and role(s) of the parties involved, and the expected behaviour(s) of the parties involved as seen by other parties involved in (electronic) learning transactions. Such rules are applied to: (a) content of the information flows in the form of precise and computer-processable meaning, i.e. the semantics of data; and, (b) the order and behaviour of the information flows themselves. NOTE 4 Rules must be clear and explicit enough to be understood by all parties to a learning transaction. Rules also must be capable of being able to be specified using a using a Formal Description Technique(s) (FDTs). EXAMPLE A current and widely used FDT is "Unified Modelling Language (UML)". NOTE 5 Specification of rules in an Open-edi transaction should be compliant with the requirements of ISO/IEC 15944-3 "Open-edi Description Techniques (OeDT)".	règle	02	énoncé régissant une conduite, une procédure, des conditions ou des rapports NOTE 1 Les règles spécifient les rapports entre les objets et leurs attributs. NOTE 2 Les règles sont de nature obligatoire ou conditionnelle. NOTE 3 Les règles spécifient formellement les engagements et le(s) rôle(s) des parties concernées, et le(s) comportement(s) prévu(s) des parties concernées tels que perçus par d'autres parties concernées par des transactions (électroniques) d'apprentissage. Ces règles s'appliquent aux éléments suivants: (a) contenu des flux d'information sous forme de signification précise et traitable par ordinateur, c.-à-d. la sémantique des données; et, (b) l'ordre et le comportement des flux d'information eux-mêmes. NOTE 4 Les règles doivent être suffisamment claires et explicites pour être comprises par toutes les parties d'une transaction d'apprentissage. En même temps, les règles doivent pouvoir être spécifiées en utilisant une ou des technique(s) de description formelle(s) (FDT). EXEMPLE L'une des techniques de description formelles actuellement et couramment utilisées est l'UML (Langage de modélisation unifié ou Unified Modelling Language). NOTE 5 Les spécifications des règles dans une transaction d'EDI-ouvert doivent être conformes aux exigences de l'ISO/IEC 15944-3 «Techniques de description de l'EDI-ouvert (OeDT)».
3.139	ISO/IEC 15944-2:2006 (3.102)	rulebase	99	pre-established set of **rules** which interwork and which together form an autonomous whole NOTE One considers a rulebase to be to rules as database is to data.	base de règles	02	ensemble préétabli de **règles** qui s'appliquent en concordance et qui ensemble forment un tout autonome NOTE On considère qu'une base de règles est aux règles ce qu'une base de données est aux données.
3.140	ISO/IEC 14662: 2010 (3.26)	scenario attribute	99	formal specification of information, relevant to an **Open-edi scenario** as a whole, which is neither specific to **roles** nor to **Information Bundles**	attribut de scénario	01	spécification formelle d'une information d'intérêt pour la globalité d'un **scénario d'EDI-ouvert**, qui ne ressortit spécifiquement ni aux **rôles** ni aux **faisceaux d'informations**
3.141	ISO/IEC 15944-2:2006 (3.104)	scenario component	99	one of the three fundamental elements of a **scenario**, **namely role**, **information bundle**, and **semantic component**	composante de scénario	02	l'un des trois éléments fondamentaux d'un scénario, nommément le **rôle**, le f**aisceau d'informations**, et la **composante sémantique**

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.142	ISO/IEC 15944-2:2006 (3.105)	scenario content	99	**set of recorded information** containing **registry** entry **identifiers**, labels and their associated **definitions** and related **recorded information** posted (or reposted) in any registry for **business** objects	contenu de scénario	01	**ensemble d'information enregistrée** contenant les **identificateurs** d'entrée de **registre**, les labels, leurs **définitions** connexes, et l'**information enregistrée** connexe publiée (ou republiée) dans tout **registre** d'objets d'**affaires**
3.143	ISO/IEC 15944-2:2006 (3.106)	scenario specification attribute	99	any **attribute** of a scenario, **role**, **Information Bundle**, and/or **semantic component**	attribut de spécification de scénario	01	tout **attribut** d'un scénario, d'un rôle, d'un **Faisceau d'informations**, et/ou d'une **composante sémantique**
3.144	ISO/IEC 15944-2:2006 (3.107)	SC identifier	99	unique, linguistically neutral, **unambiguous**, referenceable **identifier** of a **Semantic Component**	identificateur de composante sémantique	01	**identificateur** unique, linguistiquement neutre, **non ambiguë** et referenceable d'un **composant sémantique**
3.145	ISO/IEC 15944-1:2011 (3.62)	seller	99	**Person** who aims to hand over voluntarily or in response to a demand, a good, service and/or right to another **Person** and in return receives an acceptable equivalent value, usually in money, for the good, service and/or right provided	vendeur	01	**Personne** qui vise à fournir, volontairement ou suite à une demande, un bien, un service et/ou un droit à une autre **Personne**, et qui reçoit en retour une valeur équivalente acceptable, habituellement en argent
3.146	ISO/IEC 29187-1 (3.146)	Semantic Component (SC)	99	unit of **recorded information** unambiguously defined in the context of the learning goal of the **learning transaction** NOTE 1 A SC may be atomic or composed of other SCs. NOTE 2 Adapted from ISO/IEC 14662.	composante sémantique (SC)	02	unité d'**information enregistrée** définie de manière non ambiguë dans le contexte de l'objectif d'apprentissage d'une **transaction d'apprentissage** NOTE 1 Un SC peut être atomique ou composé d'autres SC. NOTE 2 Adapté de l'ISO/CEI 14662.
3.147	ISO/IEC 15944-5:2008 (3.136)	semantic identifier (SI)	99	IT-interface **identifier** for a **semantic component** or other semantic for which (1) the associated context, applicable **rules** and/or possible uses as a semantic are predefined and structured and the **Source Authority** for the applicable **rulebase** is identified (as per Part 5); and (2) for which more than one or more **Human Interface Equivalents (HIEs)** exist NOTE The identifier for a Semantic Component (SC), an Information Bundle (IB) and/or an ID Code for which one or more Human Interface Equivalents (HIEs) exist are considered to have the properties or behaviours of semantic identifiers.	identificateur cateur sémantique (SI)	01	**identificateur** d'interface TI d'une **composante sémantique** ou d'une autre sémantique pour lequel (1) le contexte qui s'y rattache, les **règles** applicables et/ou les utilisations possibles comme sémantique sont prédéfinies et structurées, et l'**Autorité de source** de la **base de règles** applicable est identifiée, et (2) existe un ou plusieurs **Équivalents d'interface humaine (HIEs)** NOTE L'identificateur d'une Composante sémantique (SC), d'un Faisceau d'informations (IB) et/ou d'un Code ID pour lequel un ou plusieurs Équivalents d'interface humaine (HIEs) sont considérés comme ayant les propriétés ou les comportements d'identificateurs sémantiques.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.148	ISO/IEC 15944-5:2008 (3.137)	set of recorded information (SRI)	99	**recorded information** of an **organization** or **public administration**, which is under the control of the same and which is treated as a unit in its information life cycle NOTE 1 A SRI can be a physical or digital document, a record, a file, etc., that can be read, perceived or heard by a Person or computer system or similar device. NOTE 2 A SRI is a unit of recorded information that is unambiguously defined in the context of the business goals of the organization, i.e., a semantic component. NOTE 3 A SRI can be self-standing (atomic), or a SRI can consist of a bundling of two or more SRIs into another “new” SRI. Both types can exist simultaneously within the information management systems of an organization.	ensemble d’information enregistrée (SRI)	01	**informations enregistrées** relatives à une **organisation** ou à une **administration publique** qui en assure le contrôle et qui sont traitées comme une unité pour ce qui a trait au cycle de vie NOTE 1 Un SRI peut être un enregistrement ou un document physique ou numérique, un dossier, un fichier, etc., qui peut être lu, perçu ou entendu par une personne, un système informatique ou un dispositif semblable. NOTE 2 Un SRI est une unité d’information enregistrée qui est définie sans ambiguïté dans le contexte des objectifs d’affaires de l’organisation, c.-à.-d. une composante sémantique. NOTE 3 Un SRI peut être une unité autonome (atomique). Il peut s’agir de deux SRI ou plus regroupés dans un « nouvel » SRI . SRI. Les deux types d’SRI peuvent exister simultanément dans les systèmes de gestion de l’information d’une organisation.
3.149	ISO/IEC 15944-2:2006 (3.109)	Source Authority (SA)	99	**Person** recognized by other **Persons** as the authoritative source for a set of **constraints** NOTE 1 A **Person** as a Source Authority for internal constraints may be an individual, organization, or public administration. NOTE 2 A **Person** as Source Authority for external constraints may be an organization or public administration. EXAMPLE In the field of air travel and transportation, IATA as a Source Authority, is an "organization," while ICAO as a Source Authority, is a "public administration". NOTE 3 A **Person** as an individual shall not be a Source Authority for external constraints. NOTE 4 Source Authorities are often the issuing authority for identifiers (or composite identifiers) for use in **learning transaction**s. NOTE 5 A Source Authority can undertake the role of Registration Authority or have this role undertaken on its behalf by another **Person**. NOTE 6 Where the sets of constraints of a Source Authority control a coded domain, the SA has the role of a coded domain Source Authority.	Autorité de source (AS)	02	**Personne** reconnue par d’autres **Personnes** comme source faisant autorité pour un ensemble de **contraintes** NOTE 1 Une personne comme Autorité de source pour des contraintes internes peut être un individu, une organisation ou une administration publique. NOTE 2 Une personne comme Autorité de source pour des contraintes externes peut être une organisation ou une administration publique. EXEMPLE Dans le domaine du transport aérien, l’IATA, comme Autorité de source, est une « organisation », tandis que l’OACI en tant qu’Autorité de source est une « administration publique ». NOTE 3 Une Personne en tant qu’individu ne peut être une Autorité de source pour des contraintes externes. NOTE 4 Les Autorités de source sont souvent les autorités émettrices des identificateurs (ou des identificateurs composites) à utiliser dans les transactions d’affaires. NOTE 5 Une Autorité de source peut jouer le rôle d’un organisme d’enregistrement ou faire jouer ce rôle à sa place par une autre Personne. NOTE 6 Lorsque l’ensemble de contraintes d’une Autorité de source contrôle un domaine codé, l’AS joue le rôle d’Autorité de source d’un domaine codé.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.150	ISO 1087-1:2000 (3.1.3)	special language	99	**language** for special purposes (LSP), **language** used in a subject field and characterized by the use of specific linguistic means of expression NOTE The specific linguistic means of expression always include subject-specific terminology and phraseology and also may cover stylistic or syntactic features.	langue de spécialité	02	**langue** spécialisée utilisée dans un domaine et caractérisée par l'utilisation de moyens d'expression linguistique spécifiés NOTE Les moyens d'expression linguistique spécifies incluent toujours une terminologie et une phraséologie propres au domaine et peuvent également couvrir des tournures stylistiques ou syntaxiques.
3.151	ISO/IEC 15944-1:2002 (3.64)	standard	99	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 NOTE This is the generic definition of "standard" of the ISO and IEC (and found in the ISO/IEC JTC1 Directives, Part 1, Section 2.5:1998). {See also ISO/IEC Guide 2: 1996 (1.7)}	norme	02	accord documenté contenant des spécifications techniques ou autres critères précis destinés à être utilisés systématiquement en tant que **règles**, lignes directrices ou **définitions** de **caractéristiques** pour assurer que des matériaux, produits, **processus** et services sont aptes à leur emploi NOTE Cette définition est la définition «normalisée» par l'ISO et la CEI (et qui se trouve dans la Directives de l'ISO/CEI JTC1, Partie 1, Section 2.5:1998). {voir aussi le Guide 2:1996 (1.7) de l'ISO/CEI}
3.152	ISO 1087: 2000 (5.3.1.2)	term	99	**designation** of a defined concept in a **special language** by a linguistic expression NOTE A term may consist of one or more words i.e. simple term, or complex term or even contain symbols.	terme	01	**désignation** au moyen d'une unité linguistique d'une notion définie dans une **langue de spécialité** NOTE Un terme peut être constitué d'un ou de plusieurs mots (terme simple ou terme complexe) et même de symboles.
3.153	ISO/IEC 2382-23:1994 (23.01.01)	text	99	**data** in the form of **characters**, symbols, words, phrases, paragraphs, sentences, tables, or other **character** arrangements, intended to convey a meaning and whose interpretation is essentially based upon the reader's knowledge of some natural language or artificial language EXAMPLE A business letter printed on paper or displayed on a screen.	texte	01	**données** sous forme de **caractères**, de symboles, de mots, d'expressions, de paragraphes, de phrases, de tableaux ou d'autres arrangements de **caractères**, ayant une signification particulière, dont l'interprétation dépend essentiellement de la connaissance de la part du lecteur d'un langage naturel ou d'un langage artificiel EXEMPLE Une lettre commerciale imprimée sur papier ou affichée à l'écran.
3.154	ISO/IEC 29187-1 (3.154)	third party (in LET privacy protection)	99	**Person** besides the two primarily concerned in a **learning transaction** who is **agent** of neither and who fulfils a specified **role** or function as mutually agreed to by the two primary **Persons** or as a result of **external constraints** NOTE 1 It is understood that more than two Persons can at times be primary parties in a learning transaction. NOTE 2 Adapted from ISO/IEC 15944-1.	tierce partie (dans la protection de la vie privée concernant l'AÉF)	02	**Personne**, autre que les deux **Personnes** concernées en premier lieu par une **transaction d'apprentissage** et qui n'est le mandataire d'aucune d'elles, et qui joue un **rôle** ou remplit une fonction spécifiés, selon l'accord mutuel des deux **Personnes** concernées en premier lieu, ou le résultat de **contraintes externes** NOTE 1 Il est entendu que plus de deux Personnes peuvent parfois être les parties de première part dans une transaction d'apprentissage NOTE 2 Adapté de l'ISO/CE1 15944-1.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.155	ISO/IEC 15944-5:2008 (3.144)	treaty	99	international agreement concluded between **jurisdictional domains** in written form and governed by international law NOTE 1 On the whole a treaty is concluded among UN member states. NOTE 2 Treaties among UN member states when coming into force are required to be transmitted to the Secretariat of the United Nations for registration or filing or recording as the case may be and for publication. {See further Article 80 or the Charter of the UN} NOTE 3 Treaties can also be entered into by jurisdictional domains other than UN member states, i.e., non-members such as international organizations and the rare sub-national units of federations which are constitutionally empowered to do so. NOTE 4 A treaty can be embodied in a single instrument or in two or more related instruments and whatever it particular designations. However, each treaty is a single entity. NOTE 5 Jurisdictional domains can make agreements which they do not mean to be legally binding for reasons of administrative convenience or expressions of political intent only, (e.g., as a Memorandum of Understanding (MOU)). NOTE 6 Adapted from the Vienna Convention on the Law of Treaties, 1(a).	traité	01	accord international conclu par écrit entre des **domaines juridictionnels** et régi par le droit international NOTE 1 Virtuellement, tous les traités sont conclus entre des états membres de l'ONU. NOTE 2 Les traités entre les états membres de l'ONU, lorsqu'ils entrent en vigueur, doivent être transmis au Secrétariat des nations unies pour être enregistrés et classés ou déposés selon le cas, et publiés. {Voir plus loin l'Article 80 ou la Charte de l'ONU} NOTE 3 Les traits peuvent également être conclus entre des domaines juridictionnels autres que les états membres de l'ONU, c.à.d., des organisations internationales et les rares organismes fédérés infranationaux qui en ont constitutionnellement le pouvoir. NOTE 4 Un traité peut être concrétisé en un seul instrument ou en plusieurs instruments lies et quelles que soient ses appellations particulières. Chaque traité, cependant, est une entité unique. NOTE 5 Des domaines juridictionnels peuvent conclure des accords qu'ils n'ont pas l'intention de rendre légalement obligatoires pour des raisons de commodité administrative ou pour exprimer une intention politique uniquement, (par ex. comme dans le cas d'un protocole d'entente). NOTE 6 Adapté de la Convention de Vienne sur le droit des traités, 1(a)
3.156	ISO/IEC 15944-5:2008 (3.145)	truncated name	99	short form of a **name** or **persona** of a **Person** resulting from the application of a **rule**-based truncation **process**	nom tronqué	01	forme abrégée du **nom** ou **persona** d'une **Personne** résultant de l'application d'un processus de troncation à base de **règle**
3.157	ISO/IEC 15944-5:2008 (3.146)	truncated recognized name (TRN)	99	**truncated name**, i.e., **persona**, of a **Person** which has the properties of a **legally recognized name (LRN)** NOTE 1 Truncated recognized name(s) may be required for use in machine-readable travel documents, (e.g., passports or visas), identity tokens, drivers' licenses, medicare cards, etc.). NOTE 2 The source of a truncated recognized name may be a legally recognized name.	nom reconnu tronqué (NRT)	01	**nom** tronqué, c.-à.-d., **persona** d'une **Personne** qui a les propriétés d'un **nom légalement reconnu (NLR)** NOTE 1 Un (ou des) nom(s) reconnu(s) tronqué(s) peut(peuvent) être exigé(s) dans l'utilisation des documents de voyage lisibles optiquement (par ex. passeports ou visas, jetons d'identité, permis de conduire, cartes d'assurance-maladie, etc.). NOTE 2 La source d'un nom reconnu tronqué peut être un nom légalement reconnu.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.158	ISO/IEC 15944-5:2008 (3.147)	truncation	99	**rule**-base **process**, explicitly stated, for shortening an existing **name** of an **entity** to fit within a predefined maximum length (of **characters**) NOTE Truncation may be required for the use of names in IT systems, electronic data interchange (EDI), the use of labels in packaging, in the formation of a **Person** identity (Pi), etc.	troncation	02	**processus** à base de **règle**, énoncé explicitement, pour raccourcir le **nom** existant d'une **entité** de façon à ne pas dépasser une longueur de **caractères** maximum prédéfinie NOTE Une troncation peut s'avérer nécessaire pour l'utilisation de noms dans les systèmes TI, l'échange de données informatisées (EDI), les étiquettes d'emballage, la formation de l'identité d'une personne (Pi), etc.
3.159	ISO/IEC 29187-1 (3.159)	unambiguous (in LET privacy protection)	99	level of certainty and explicitness required in the completeness of the semantics of the **recorded information** interchanged appropriate to the goal of a **learning transaction** Note Adapted from ISO/IEC 15944-1.	non-ambigu (dans la protection de la vie privée concernant l'AÉF)	03	niveau de certitude et d'explicité exigé dans la complétude de la sémantique d'une **information enregistrée** et échangée dans le but d'une **transaction d'apprentissage** NOTE Adapté de l'ISO/CE1 15944-1.
3.160	ISO/IEC 29187-1 (3.160)	vendor	99	**seller** on whom **consumer protection** requirements are applied as a set of **external constraints** on a **learning transaction** NOTE 1 Consumer protection is a set of explicitly defined rights and obligations applicable as external constraints on a **learning transaction**. NOTE 2 It is recognized that external constraints on a seller of the nature of consumer protection may be peculiar to a specified jurisdictional domain. Note Adapted from ISO/IEC 15944-1.	fournisseur	01	**vendeur** auquel s'appliquent des exigences de **protection des consommateurs** comme ensemble de **contraintes externes** sur une **transaction d'apprentissage** NOTE 1 La protection des consommateurs est un ensemble de droits et d'obligations explicitement définis, et qui s'appliquent comme contraintes externes à une transaction d'apprentissage. NOTE 2 On reconnaît que les contraintes externes, telles que la protection des consommateurs, exercées sur un fournisseur, peuvent relever d'une juridiction particulière. NOTE Adapté de l'ISO/CE1 15944-1
3.161	ISO 1087-1:2000 (13.7.2)	vocabulary	99	terminological **dictionary** which contains **designations** and **definitions** for one or more specific subject fields NOTE The vocabulary may be monolingual, bilingual or multilingual.	vocabulaire	01	**dictionnaire** terminologique contenant des **désignations** et des **définitions** tirées d'un ou plusieurs domaines particuliers NOTE Un vocabulaire peut être unilingue, bilingue ou multilingue.

[THIS PAGE IS INTENTIONALLY LEFT BLANK]

Annex B
(normative)

Learning Transaction Model (LTM): classes of constraints

B.1 Introduction

On the whole one models modules or specifies requirements in the form of “constraints”. These can be of a nature of rules (or guidelines), definition of concepts, a predefined set of permitted choices, (e.g., as coded domains).

This multipart ISO/IEC 29187 standard focuses on supporting privacy protection requirements in an ITLET context. Privacy protection requirements apply when an individual and an organization or public administration agree[106)] o engage in a learning transaction.

The purpose of this Annexes is to state these requirements. On the whole these are based on existing international ISO standards.

B.2 Fundamental components of a learning transaction

Learning transactions can be modelled for registering, reference and re-use as scenarios and scenario components. Business semantic descriptive techniques can used to identify and specify the key components of a learning transaction, i.e., as learning objects (or LET objects)[107)] The Learning Transaction Model (LTM) has three required components namely "Person", "Process", and "Data. These three fundamental components are presented graphically in Figure B.1[108)] This is because both a business transaction and a learning transaction are sub-types of an agreed upon commitment exchange among autonomous parties.

[106)] At times, external constraints require, i.e., mandate, the participation of an individual learner in various learning transactions, (e.g., K-12 legislated requirements requiring an individual form age 5-6 to 17-18 to participate in a LET activity).

[107)] The rules in this classes of ISO/IEC 15944-1:2010 apply here to Annex B also. They have been adapted in a LET context.

[108)] In ISO/IEC 15944-1:2010 for these three fundamental elements, are the essential BOV aspects of the learning transaction model, along with associated rules, definitions and terms as well as other attributes are stated in the following clauses:

(1) Clause 6.2 "Rules governing the Person Component" (and further Annex E);

(2) Clause 6.3 "*Rules governing the Process Component"* (and further Annex F); and,

(3) Clause 6.4 *"Rules governing the Data Component"* (and further Annex G).

Rule B-001:
Any learning transaction has three fundamental components[109] namely: (1) a "Person" (as a whole or per its three sub-types of individual, organization, or public administration in the privacy party to any commitment exchange including that of the nature of a learning transaction.

(Graphic illustration)

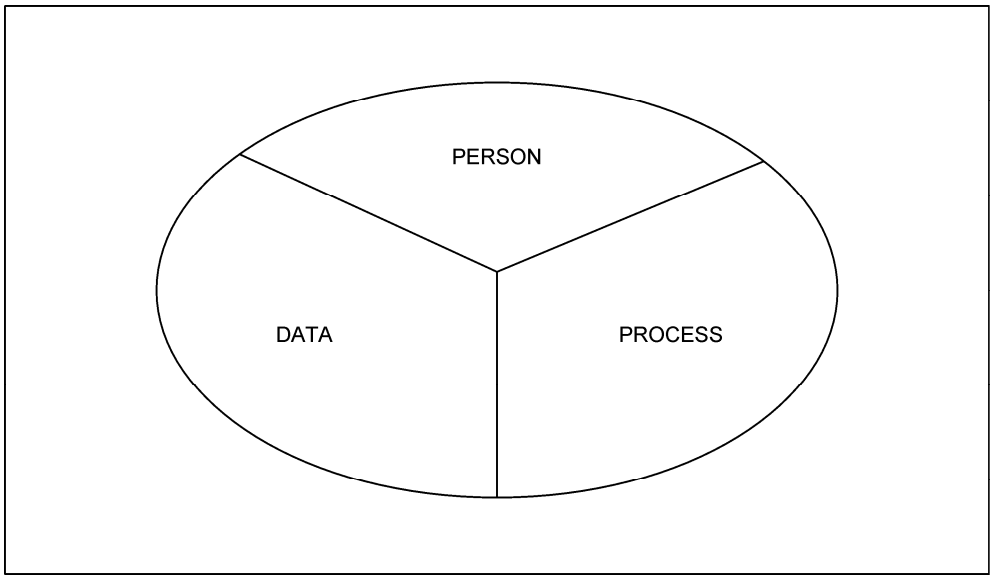

Figure B.1 — Learning Transaction Model – Fundamental components

Using UML as a Formal Description Technique yields the following UML-based representation of the Learning Transaction Model and is presented as Figure B.2.[110]

[109] Most of the existing ISO/IEC JTC1 standards as well as many of the existing ISO, IEC or ITU standards (including those referenced in Clause 2 above) do not or were not designed to be able to address any two or more of the "Person", data and/or process components in an integrated manner.

[110] This UML-based representation incorporates the rules governing the interworking of these three fundamental components as specified in ISO/IEC 15944-1:2010.

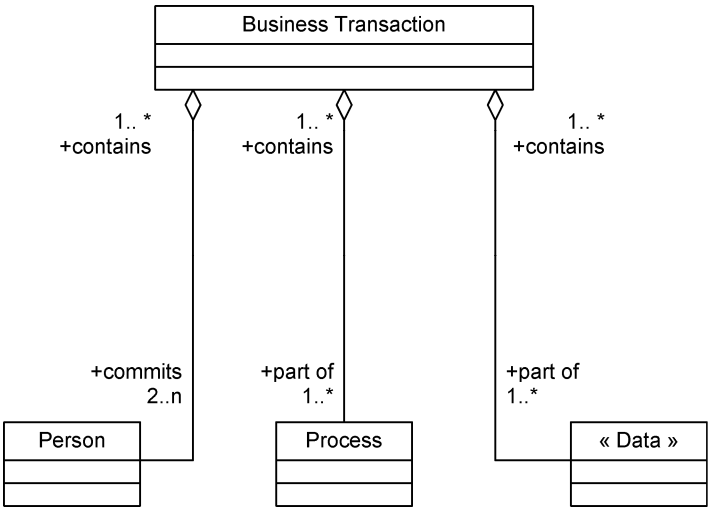

Figure B.2 — UML-based Representation of Figure B.1 – Learning Transaction Model

The learning transaction model (LTM) focuses on and addresses the essential needs of commitment exchange among autonomous parties, i.e., the ability of Persons as parties to a learning transaction being able to make commitments and to do so while maximizing the use of automated methods. This is in addition to existing standards which pertain to various aspects of information exchange only.[111)] As such, what sets Open-edi apart from information exchange in general are six (6) characteristics[112)]

They are:

- actions based upon following clear, predefined rules;
- commitments of the parties involved;
- commitments among the parties are automated;
- parties control and maintain their states;
- parties act autonomously; and,
- multiple simultaneous transactions can be supported.

Electronic learning transactions therefore require:

1) a clearly understood purpose, mutually agreed upon goal(s) explicitness and unambiguity;

2) pre-definable set(s) of activities and/or processes, pre-definable and structured data;

3) commitments among Persons being established through electronic data interchange;

---

111) It is important that users of this part of ISO/IEC 15944 familiarize themselves with Part 1, Clause 6.3.1 titled *"Learning transactions commitment exchange added to information exchange*" including the rules and definitions/terms, i.e., "Person", and "commitment" as well as its normative text.

112) See further in ISO/IEC 15944-1:2010 Clause 5 "*Characteristics of Open-edi",* where of these six (6) characteristics is described in more detail.

4) computational integrity and related characteristics; and,

5) the above being specifiable through Open-edi Description Technique(s) (OeDTs) (as the use of a Formal Description Technique(s) in support of modelling e-business), and executable through information technology systems for use in real world actualizations.

These and related requirements of electronic learning transactions are specified in the form of "constraints".

"Constraint" has already been defined in ISO standards. The existing ISO definition has been adapted in a LET context as follows:

constraint

rule, explicitly stated, that prescribes, limits, governs or specifies any aspect of a **learning transaction**

NOTE 1 Constraints are specified as rules forming part of components of Open-edi scenarios, i.e., as scenario attributes, roles, and/or sets of recorded information (SRIs).

NOTE 2 For constraints to be registered for implementation in Open-edi, they must have unique and unambiguous identifiers.

NOTE 3 A constraint may be agreed to among parties (condition of contract) and is therefore considered an "internal constraint". Or a constraint may be imposed on parties, (e.g., laws, regulations, etc.), and is therefore considered an "external constraint". [adapted from ISO/IEC 15944-1:2010:3.11]

B.3 Learning Transaction Model (LTM) and its two classes of constraints

The Learning Transaction Model has two classes of constraints; namely,

1) those which are "self-imposed" and agreed to as commitments among the parties themselves, i.e., "**internal constraints**"; and,

2) those which are imposed on the parties to a learning transaction based on the nature of the LET good, service and/or rights exchanged, the nature of the commitment made among the parties (including ability to make commitments, the location, etc.), i.e., "**external constraints**".

The concept of “internal constraint” has already been defined in existing ISO standards. It has been adapted in a LET context as follows:

internal constraint
constraint *which forms part of the* ***commitment(****s) mutually agreed to among the parties to a* ***learning transaction***

NOTE Internal constraints are self-imposed. They provide a simplified view for modeling and re-use of scenario components of a learning transaction for which there are no external constraints or restrictions to the nature of the conduct of a learning transaction other than those mutually agreed to by the buyer and seller.

[adapted from ISO/IEC 15944-1:2010, 3.033]

The concept of “external constraint” has already been defined in existing ISO standards. It has been adapted in a LET context as follows:

> ***external constraint***
> ***constraint which takes precedence over internal constraints in a learning transaction, i.e., is external to those agreed upon by the parties to a learning transaction***
>
> NOTE 1 Primary sources of external constraints are created by law, regulation, orders, treaties, conventions or similar instruments.
>
> NOTE 2 Other sources of external constraints include those of a sectoral nature, those which pertain to a particular jurisdiction or a mutually agreed to common business conventions, (e.g., INCOTERMS, exchanges, etc.).
>
> NOTE 3 External constraints can apply to the nature of the LET good, service and/or right provided in a learning transaction.
>
> NOTE 4 External constraints can demand that a party to a learning transaction meet specific requirements of a particular role.
>
> EXAMPLE 1 Only a qualified medical doctor may issue a prescription for a controlled drug;
>
> EXAMPLE 2 Only an accredited share dealer may place transactions on the New York Stock Exchange;
>
> EXAMPLE 3 Hazardous wastes may only be conveyed by a licensed enterprise.
>
> NOTE 5 Where the sets of recorded information (SRIs), including their Semantic Components (SCs) of a learning transaction form the whole of a learning transaction, (e.g., for legal or audit purposes), all constraints must be recorded.
>
> EXAMPLE There may be a legal or audit requirement to maintain the complete set of recorded information pertaining to a learning transaction (the SRIs exchanged), as a "record".)
>
> NOTE 6 A minimum external constraint that is often applicable to a learning transaction requires one to differentiate whether the Person, i.e., that is a party to a learning transaction, is an "individual", "organization", or "public administration".
>
> EXAMPLE Privacy rights apply only to a Person as an "individual".
>
> [adapted from ISO/IEC 15944-1:2010, 3.023]

The class of "internal constraints" has been derived to provide a simplified view of learning transactions for which there are no external constraints or restrictions to the nature and conduct of the transaction. The only constraints are those mutually agreed to by the buyer and LET provider for the explicitly stated goal of the learning transaction, i.e., they are self-imposed. This allows one to build scenarios and scenario components for referencing, registering and re-use as generic or base scenarios without having to include potential external constraints. The rules governing specification of Open-edi scenarios and their components require that all applicable external constraints must be stated at the time of instantiation but need not exist at the time of registration. {See further, Clause 9 in ISO/IEC 15944-1:2010 and its Annex I}

However, in most learning transactions, external constraints do apply, i.e., applicable laws and regulations. These range from education related regulation and professional requirements; health and safety or packaging and labelling requirements; ensuring that nature of the learning transaction and/or the goods or services delivered do not comprise behaviour of a criminal nature. Whilst laws and regulations exist within and among jurisdictions and are the primary source of "external constraints" on learning transactions, categorization and specification of sub-classes of external constraints is outside the scope of this standard.

External constraints exist which are horizontal in nature. These are the common and generic rules for learning transactions, (e.g., privacy/data protection, consumer policy, uniform professional codes, etc.).

The imposition of these horizontal external constraints on learning transactions is exemplified by the introduction of a third type of role in a learning transaction, namely that of “regulator” as a third sub-type of Person as a player in a learning transaction representing "public administration".

External constraints of a horizontal and common nature are constraints imposed by regulators (and enacted through public administrations) which apply regardless of the type of business or sector within which the business occurs. This categorization allows one to build scenarios and scenario components for referencing, registering and reuse of specific common sets of external constraints. These can then be combined with scenarios which focus on internal constraints for building application use scenarios.

There are also external constraints that are of a sectoral nature. In addition, some external constraints can be common to two or more sectors and supported through common standards. Sectoral constraints are found in LET, telecommunications, transportation and delivery, financial/banking, import/export restrictions specific to a good or service, inter-or intra-state trade, and so on. Where a sector imposes specific ways of conducting learning transactions within itself and with other sectors, such sector specific constraints and conditions must be identified and specified where applicable, as part of specification of scenarios and scenario components.[113)] This allows one to build scenarios and scenario components for referencing, registering and reuse of sets of sectoral external constraints such as “customs clearance”, “transport of dangerous goods”[114)] , etc. These two basic classes of constraints on learning transactions are illustrated below in Figure B.3: Learning Transaction Model: Classes of Constraints.

These two basic classes of constraints on learning transactions are illustrated here in Figure B.3.

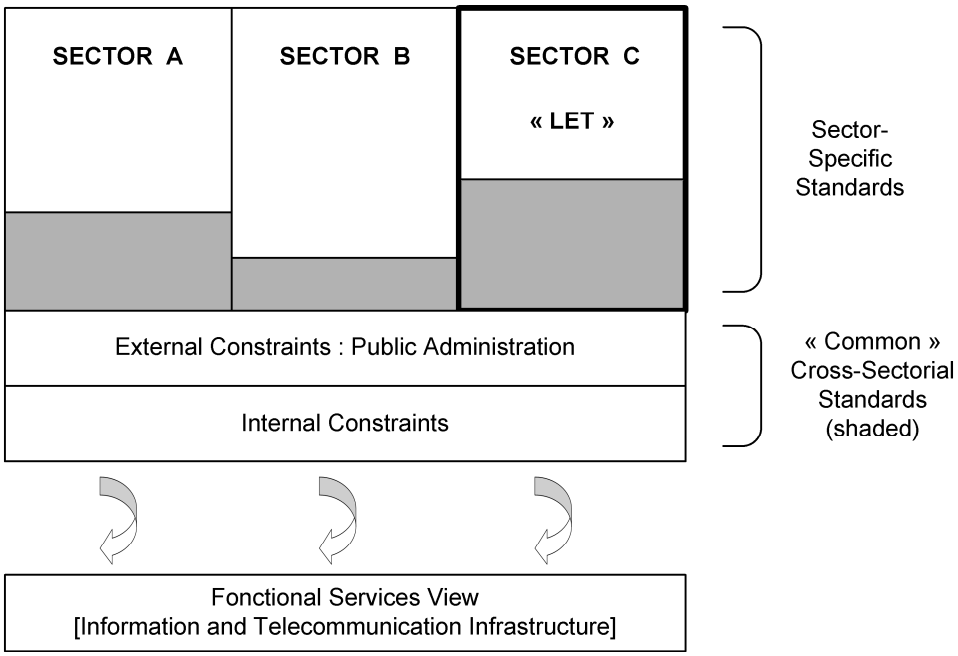

Figure B.3 — Learning Transaction Model: Classes of constraints

---

[113)] A useful characteristic of external constraints is that at the sectorial level, national and international focal points, recognized authorities often already exist. The rules and common business practices in many sectorial areas are already known. Use of this standard (and related standards) will facilitate the transformation of these external constraints (business rules) into specified, registered and re-useable scenarios and scenario components.

[114)] Note: There are also requirements for establishing common rules for interchanges between as well as among sectors. These rules are normally imposed by a particular sector on the others. For example, the banking sector may impose certain rules for the exchange of financial information between itself and other sectors. Sometimes the rules are established to enhance or facilitate services of a particular sector with others. The transportation sector is a good example. It establishes business rules in conjunction with other sectors for the transport and handling of specialty goods, (e.g., radioactive materials, live animals, etc.).

Annex C
(normative)

Integrated set of information life cycle management (ilcm) principles in support of information law compliance

C.1 Introduction

From a learning transaction perspective, one deals only with recorded information. Privacy/data protection is part of a set of public policy requirements which include consumer protection, individual accessibility, human rights, etc.

Further, there are also generic legal requirements which pertain to any sets of recorded information (SRIs) interchanged among parties to a learning transaction. These include record retention requirements, those of an evidentiary nature, archiving, contingency/disaster planning, etc., a.k.a., “information law” requirements, governing information management and data interchange of an organization.

The purpose of this Annex C is to consolidate these operational view requirements (including those of an external constraints nature) into a single set of high level or “primitive” principles. Having such a short Annex in ISO/IEC 29187-1 (including the concept and definition of “information law”) will facilitate the further development of Part 1 Framework and Reference Model as well as its additional Parts 2+. This is because these ILCM principles will provide a generic context and reference for information management and data interchange requirements including those required to support privacy protection requirements.

C.2 Purpose

The procedures, documentation and related activities pertaining to learning transactions and resulting sets of recorded information (consisting of one or more SRIs) require that the highest standards of date integrity and trustworthiness are maintained. A primary factor here is that learning transactions represent the most common form of making and executing commitments among the parties to the learning transaction.

These common requirements pertain not only to the flows of information and the contents of the recorded information but those which exist in support of many other laws, regulations, etc., impacting information management and interchange as well as supporting documentation. Examples of such laws impacting learning transactions include those pertaining to records keeping, access and use, disposition, archiving, etc. These are stated in the form of laws, pursuant regulations, statutory instruments, policies, codes, etc. They are of a generic "information law" nature. Information law is defined as:

> ***information law***
> *any law, regulation, policy, or code (or any part thereof) that requires the creation, receipt, collection, description or listing, production, retrieval, submission, retention, storage, preservation or destruction of* ***recorded information****, and/or that places conditions on the access and use, confidentiality, privacy, integrity, accountabilities, continuity and availability of the processing, reproduction, distribution, transmission, sale, sharing or other handling of* ***recorded information****.*
>
> [ISO/IEC 15944-8:2011, 3.062]

It is (totally) outside the scope of this multipart standard to identify all the information law requirements applicable to the recorded information of any kind under the control of an organization (or public administration).

The purpose of this Annex C is to bring forward a high **level set of generic information life cycle management (ILCM) principles** which integrate and consolidate the essential elements of any law, regulation, etc., which has an information law component(s). These principles are generic in nature. On the whole they apply to both internal constraints and external constraints. These ILCM principles therefore also provide an overall context in support of the privacy protection principles presented in Clause 5 above.

C.3 Approach

From a high level perspective, and taking into account federal and provincial/territorial, generic and sector specific information law requirements of jurisdictional domains (as well as those pertaining to access, privacy, confidentiality, security, etc.), one can group these ILCM requirements into a number of discrete categories.

Discrete categories of "information law" already identified include those that:

1) require one to keep or retain certain recorded information;

2) require one to have the ability to produce or retrieve certain types of recorded information;

3) require one to submit or file recorded information to a government or regulatory agency;

4) require one to create and/or make available recorded information if one undertakes a particular activity, i.e., pertaining to a product, service and/or right;

5) require one retain recorded information “indefinitely” or for a specified period of time;

6) require one to destroy recorded information;

7) place conditions on access, use and/or confidentiality of recorded information;

8) place conditions on the manner in which one handles recorded information;

9) place conditions on the reproduction, distribution or sale of recorded information;

10) place conditions on the sharing, linking or flows of recorded information (within or among jurisdictions); and,

11) require “public” release/disclosure of certain recorded information (a priori or on request).

With respect to these categories:

1) one or more of these categories of information law can apply to a "set of recorded information (SRI); and,

2) an "information law" can include more than one category of requirements.

C.4 Integrated set of information life cycle management (ILCM) principles

Given the definition of "information law" and the examples of categories of information law already identified, any user or implementer of this standard can quickly identify ten (10) or more different laws and regulations of an "information law" nature which apply to the recorded information forming part of a learning transaction.

Two basic approaches are possible. The first, which is the current, traditional approach, is that of addressing each information law requirement on its own, i.e., as a "vertical silo". Here different operational areas within an organization comply with information law requirements on their own, integrate them into their applications, and deal with issues as they are identified, a crisis occurs, an audit discovers gaps, lack of compliance results in court actions, liability suits, etc. Convergence in and information communication technologies (ICT), increased the need for trustworthiness and integrity, accountability, etc., has made this "traditional" approach increasingly less viable.

It is vital that such an integrated approach to information life cycle management of the recorded information of an organization be senior management approved and driven. It is also very important that such ILCM principles focus on the WHATs not the HOWs and be stated in simple, non-technical language.

The eight (8) key Information Life Cycle Management (ILCM) Principles presented here incorporate a wide variety of information law requirements common to most jurisdictional domains as well as widely accepted best management practices of an "organization". They are:

1) Any "recorded information" which exists at an organization must be directly relatable to, and be in support of, an authorized mandate, program, delivery of product and/or service, (research) project, administrative mandate, or other specified and approved activity of the organization.

2) Any organization (for-profit or not-for-profit basis) or public administration must have: (a) an accurate and up-to-date list of all information law requirements which apply to the organization, i.e., both of a generic horizontal nature and those specific to the mix of goods and/or services it provides; and, (b) must be in full compliance with such information law requirements.

3) All recorded information must be timely, accurate and relevant, and under "control", i.e., it must be identifiable, retrievable and accountabilities must be assigned.

4) Information management policies and practices, as well as those for supporting information handling systems, must ensure the level of trustworthiness, (data) integrity, quality and dependability is consistent with and supports the organization's objectives and information law requirements.

5) Where warranted, recorded information should be protected from premature and/or non-authorized disclosure. Adequate safeguards must be enacted to ensure the required levels of confidentialities.

It is important to note that the corollary of this policy principle, i.e., mandated disclosure, is supported equally. That is, recorded information, to which the public in general and/or specified Persons have a right of access to, must not be withheld from disclosure.

6) Recorded information which has long-term value and/or forms part of the corporate memory should be identified and conserved. This includes recorded information required for contingency planning, back-up, emergency response and related requirements.

7) Recorded information which may have historical value should be identified and conserved (as part of the organization's and/or public administration's electronic cultural heritage/«patrimoine informatisée»).

8) Any recorded information which is no longer relevant to an organization's operations and which does not meet the above criteria shall be disposed of immediately.

[THIS PAGE IS INTENTIONALLY LEFT BLANK]

Annex D
(normative)

Coded domains for specifying state change and record retention management in support of privacy protection requirements

D.1 Introduction

Generic aspects of external constraints of jurisdictional domains as rules governing learning transactions are found in ISO/IEC 15944-5 and those with respect to privacy protection requirements for Annex F (normative) of ISO/IEC 15944-8[115)]

Within a data management and interchange context, it is important that parties to a learning transaction control the states of their IT systems. This is a fundamental characteristic of Open-edi. Under internal constraints it is a best practice of organizations and public administrations to maintain control of the sets of recorded information in their IT systems (as especially those in their DMAs). This includes both state changes and records retention requirements. This pertains to basic information life cycle management (ILCM) principles in support of information law compliance. {See further above Annex C}

The need for information law compliance is even more so and mandatory when the set(s) of recorded information pertain to a learning transaction, i.e., a "commitment exchange", where the buyer is an individual learner and the seller is a LET provider. This is because privacy protection requirements apply as external constraints and make ILCM principles mandatory.

These generic Open-edi aspects and rules pertaining to a learning transaction are mandatory in any learning transaction context which involves an individual as a buyer, i.e., the role of an individual learner. This is because where this is the case privacy protection requirements apply.

The purpose of this Annex D is therefore to bring these generic Open-edi requirements of the ISO/IEC 15944-5 and -8 ISO standards forward in the particular context of ISO/IEC 29187-1 which focuses on privacy protection requirements in a LET context; namely:

1) those pertaining to state changes in the sets of recorded information (SRIs) at whatever level of granularity; and

2) those pertaining to records retention requirements (including assured destruction) of personal information.

[115)] Note: Users of this document are advised to familiarize themselves with the rules, definitions and associated text of Clause 6.6.4 "*Data component*", as found in ISO/IEC 15944-5:2008 and Annex F (normative) as found in ISO/IEC 15944-8:2011. Both are freely available standards.

A common requirement of external constraints of a public policy nature is that they mandate records retention (and deletion) requirements, (e.g., consumer protection, privacy protection, etc. nature). In order to bridge legal, operational, public policy and IT perspectives, records retention is defined as in an Open-edi context [116] as:

> ***Open-edi records retention (OeRR***
> *specification of a period of time that a **set of recorded information** must be kept by a **Person** in order to meet operational, legal, regulatory, fiscal or other requirements as specified in the **external constraints** (or **internal constraints**) applicable to a **Person** who is a party to a **learning transaction***
>
> [adapted from ISO/IEC 15944-5:2008, 3.92]

As stated in ISO/IEC 15944-1:2010 records retention requirements need to be specified:

1) in the scoping of an Open-edi scenario, (e.g., as a Post-actualization requirement, or a Data Component requirement);

2) as an attribute of an Information Bundle, (or SRI), (e.g., for specifying internal constraints). {See ISO/IEC 15944-1 Clause 8.5.2.8 and Rule 140; and, for external constraints, see ISO/IEC 15944-1, Clause 8.5.2.9 and Rule 141}.

It is important to be able to specify which of the parties to a learning transaction is responsible for retention of SRIs interchanged as IBs including those with other parties to a learning transaction.

Many, if not most, of the privacy protection requirements are of an information management nature. A key reason here is the privacy protection requirements are a type of information law. Consequently, the integrated set of information life cycle management (ILCM) principles applies. {See further Annex C above}

Rule D-001:
Management and control of state change, retention and destruction of personal information by a LET provider shall be based on the application of the integrated set of information life cycle management (ILCM) principles.

The following two clauses in Annex D focus on the:

a) state changes and state change management of personal information; and,

b) management of record retention [117] requirements of personal information,

as part of privacy protection requirements.

---

[116] Multiple definitions exist for “records retention” within a single jurisdictional domain as well as among jurisdictional domains, professional organizations, etc. In order to differentiate the concept of “records retention” within the context of e-learning e-business, e-government, etc., a unique label or term has been invented/coined, i.e. that of “Open-edi records retention (OeRR).

[117] Another common requirement is that of security services. Here many ISO/IEC and ITU standards already exist of a FSV nature which facilitates the specification and implementation of the same based on LOV requirements.

D.2 State Changes

D.2.1 Introduction

A fundamental aspect of data management and interchange among autonomous Persons (or even within an organization or public administration) is that of ensuring the accuracy, timeliness and relevancy of its (sets of) recorded information, i.e., as SRIs. A second fundamental aspect here is that any Person (or whatever nature) shall do so in compliance with applicable external constraints of the relevant jurisdictional domain.

A key characteristic of Open-edi is that "parties control and maintain their states". {See Clause 5.4, in ISO/IEC 15944-1:2002}. As such, it is important to know whether or not the value of a SRI once recorded and possibly interchanged among parties to a learning transaction is allowed to be changed during any stage in the process component.

Knowing whether or not state changes are allowed for a specific SRI is important for the management in the IT systems of state description and automated change management of the state machines of the parties involved in an (electronic) learning transaction.

This is a requirement which also exists in modelling learning transactions involving internal constraints only. However, those which exist here are likely to be a sub-set of those which arise from external constraints.

A related issue is that of “What happens to recorded information which existed prior to a state change being made”? It is important here for parties to a learning transaction to know this. In summary, two attributes are required to specify state change of data. They are:

1) number of state changes allowed, if any; and,

2) store change type.

The inter-working of these two attributes, i.e., as codes in two coded domains, covers the various combinations of state changes in the data value for SRI pertaining to the personal information of an individual learner as well as what actions are required of a LET provider with respect to both “new” and “old” data including those required for information life cycle management (ILCM) within an organization, audit trains, evidentiary requirements and any external constraints of this nature of jurisdictional domains.

The coded domains presented below address the most primitive, i.e., essential, requirements of specifying and managing state changes (at whatever level of granularity) of SRIs in an IT system. Their primary focus is to be directed at ensuring that public policy requirements are able to be supported especially in the IT systems of a LET provider.

D.2.2 Specification of state changes allowed to personal information

Rule D-002:
Where an individual is a party to a learning transaction, i.e., as a individual learner, the LET provider (as an organization or public administration) shall have in place rules governing state changes, if any, for personal information (at whatever level of granularity required) in support of data management and interchange required to comply with privacy protection requirements.

The following coded domain from ISO/IEC 15944-5 applies here. In a LET context (1) a Semantic component (SC) is equivalent to a SRI forming part of the personal information maintained by a LET provider in the DMAs of its IT systems on an individual learner; and, (2) an Information Bundle (IB) is equivalent to those SRIs containing personal information which are interchanged by a LET provider with all the parties to a learning transaction, including the individual learner.

Table D.1 **— ISO/IEC 15944-5:05 Codes for specifying state changes allowed for the values of Information Bundles and Semantic Components**[118)]

ISO/IEC 15944-5:05 Codes for Specifying State Changes Allowed for the Values of Information Bundles and Semantic Components				
IT Interface			**Human Interface Equivalent: Linguistic –Written Form**	
Source Authority ID	**Coded Domain ID**	**ID Code**	**ISO English**	**ISO French**
15944-5	05	00	no state change allowed (default)	
15944-5	05	01	one state change allowed	
15944-5	05	02	two state changes allowed	
15944-5	05	03	three state changes allowed	
15944-5	05	04	four state changes allowed	
15944-5	05	05	five state changes allowed	
15944-5	05	06	six state changes allowed	
15944-5	05	07	seven state changes allowed	
15944-5	05	08	eight state changes allowed	
15944-5	05	09	no limit on the number of state changes allowed	

An example of use of Code “0” would be the transaction record ID number as the learning transaction identifier (LTI), {See further Clause 11.2 above} i.e., the unique ID number assigned by the LET provider to an instantiated learning transaction. Codes “1”, “2”, “3”, etc., are used to deal with IBs and SCs pertaining to location information, (e.g., physical or electronic addresses), price and terms negotiations, the individual learner changing its decision on a choice of options, etc.

An example of a SRI (or data element, IB, or SC) having a Code “09” with respect to state changes would be where the LTI pertains to a student record as a whole. Here numerous additions are allowed, to a SRI at the student record level. However, with respect to SRI serving as a single entry in a student record only a Code 01 may be valid, (e.g., where a grade assigned to completion of a course may be changed upon review (resolution of dispute), etc.

Rule D-003:
An instantiated learning transaction shall have one or more SRIs for which no state changes are permitted. One of these is to serve as the transaction ID number, i.e., a learning transaction identifier (LTI) for the instantiated learning transaction.

Guideline D003G1:
It is advised that in modelling a learning transaction and/or the SRIs pertaining to personal information on or about an individual learner that the LET provider set the state change code to “00” for all SRIs and do so at the data element level.

This Guideline serves to ensure that all parties to a learning transaction agree to and have knowledge of permitted state change to the value of a SRI.

[118)] NOTE: Should there be a requirement for additional conditions for the specification of records retention responsibilities these can be added via a Technical Corrigenda to this standard or in the next edition of this standard.

Guideline D003G2:
It is also advised that in modelling a learning transaction and/or the SRIs pertaining to personal information on or about an individual learner that the LET provider specify that if a state change is allowed for an SRI, whether (a) only the LET provider can initiate such a state change, i.e., for a SRI under its control, (e.g., a change in a course grade); (2) only the individual learner can initiate such a state change, I .e., for a SRI under its control, (e.g., a change in location as physical or electronic address of the individual learner)' and/or, (3) those which can be initiated by either the individual learner or the LET provider but which requires then common (informed consent) to such a state change.

Rule D-004:
If a state change is required, the LET provider (and/or regulator) shall specify the number of state changes permitted.

Guideline D004G1:
In support of rules D-002 and D-003, the LET provider as well as other parties to the learning transaction as applicable, (e.g., the regulator, an agent, or third party) should use the ISO/IEC 15944-5 Coded domain 05 to specify the applicable state change ID codes.

D.2.3 Store Change Type

Rule D-005:
If a state change is permitted to the original data value of the IB (or its associated SCs), i.e., (1) as originally entered in the DMA(s) of the IT system(s) of the organization or public administration which acting in the role of a LET provider or a regulatory in a learning transaction involving an individual and/or as, (2) interchanged among Persons involved in a LET transaction, it is necessary to the store change type permitted.

The most common, i.e., primitive, store change types are stated in the coded domain for "Codes Representing Store Change Type".

Guideline D-005G2:

In support of rule D-005, the LET provider as well as other parties to the learning transaction as applicable. (e.g., the regulator, an agent or a third party) should use the ISO/IEC 15944-5 Coded Domain 06 to specify store change type at the SRI level

Table D.2 — ISO/IEC 15944-5:06 Codes representing store change type for Information

[NOTE: In a learning transaction context, IBs, and SCs are considered to be SRIs Bundles and Semantic Components[119)]				
ISO/IEC 15944-5:06 Codes Representing Store Change Type for Information Bundles and Semantic Components				
IT Interface			**Human Interface Equivalent: Linguistic – Written Form**	
Source Authority	**Coded Domain ID**	**ID Code**	**ISO English**	**ISO French**
15944-5	06	00	others	autre
15944-5	06	01	store new data value and (expunge previous data value)	
15944-5	06	02	store new data value, expunge previous value with date/time stamp when state change occurred	
15944-5	06	11	store new data value and previous data value only	
15944-5	06	12	store new data value and previous data value only and add a date/time stamp	
15944-5	06	21	store new data value and “nn” previous values maintaining a sequence number of all state changes. Here “nn” must be specified	
15944-5	06	22	store new data value and “nn” previous values maintaining a date/time stamp for each state change. Here “nn” must be specified	
15944-5	06	31	store new data value and all changes maintaining a sequence number of all state changes	
15944-5	06	32	store new data value and all changes, maintain a date/time stamp for each state change	
15944-5	06	99	not applicable, i.e., no state change allowed	

One notes that a code “99” here works in tandem with a Code “00” in the previous Coded Domain. Use of a Code “01” or “02” means that having the previous value only is sufficient. This is often the case for change in location, (e.g., for physical or electronic address information). The use of the other codes links to ensuring record of decision, audit trails, evidentiary requirements and other external constraints which may apply due to the nature of the learning transaction.

D.3 Records retention

On the whole, recorded information pertaining to any type of transaction is only retained as long as it is relevant to that transaction. At the same time, a LET provider as an organization or public administration may be required to retain SRIs of a particular nature for a minimum period, (e.g., in order to comply with applicable requirements of jurisdictional domains depending on the nature and purpose for which the information in question was recorded in the first place).

[119)] NOTE: Should there be a requirement for additional conditions for the specification of records retention responsibilities these can be added via a Technical Corrigenda to this standard or in the next edition of this standard.

At the same time, privacy protection requirements on the while require the expungement of any personal information as soon as the transaction is completed, (e.g., in jurisdictional domains no later than two years after the transaction has been completed).

The rules which follow with respect to records retention facilitate a systematic approach by a LET provider to be able to support not only record retention specification requirements of a Let privacy protection requirements nature, but also those which apply to (1) any transaction which involves public policy requirements applicable to an individual as a party to that transaction; and, (2) other relevant records retention requirements of the applicable jurisdictional domain.

Rule D-006:
Where an individual participates in the role of an individual learner in a learning transaction, the LET provider shall specify who is responsible for the retention of any (combination of) set(s) of recorded information during the negotiation phase and no later than at the actualization phase in accordance with privacy protection requirements.

Rule D-007:
Where an individual participates in the role of an individual learner in a learning transaction, the LET provider shall ensure that all other parties to the instantiated learning transaction, as applicable, (e.g., a regulator, an agent, and/or third party) are informed of records retention (and destruction requirements).

Guideline D-007G1:
In support of Rules D-004 and D-005, the LET provider, as well as any other parties to the learning transaction, (e.g., a regulator, an agent, and/or third party) should use ISO/IEC 15944-5 Coded domain 02 Codes Representing Specification of Records Retention Requirements. This coded domain is presented below as Table D-3.

Within the context of collaboration space of a learning transaction, a number of basic common options exist for specifying responsibility for Open-edi records retention (OeRR) among the parties to a learning transaction. They have already been identified in the following coded domain in ISO/IEC 15944-5.

External constraints of a public policy nature such as privacy protection (and consumer protection as well) require, i.e., make mandatory, both (1) the retention of personal information pertaining to a learning transaction where the individual participates; and, (2) the assured destruction by the LET provider of personal information based on both legal requirements and contractual obligations. {See further above Annex C (Normative) Integrated set of information life cycle management (ILCM) principles in support of information law compliance}.

NOTE In a LET context, the use of this coded domain has the following equivalents.

a) seller = LET provider

b) buyer = individual learner

c) IB or SC = SRI

d) regulator = regulator.

Table D.3 **—ISO/IEC 15944-5:02 Codes Representing Specification of Records Retention Responsibility**[120)]

ISO/IEC 15944-5:02 Codes Representing Specification of Records Retention Responsibility				
IT Interface			Human Interface Equivalent: Linguistic – Written Form	
Source Authority ID	Coded Domain ID	ID Code	ISO English	ISO French
15944-5	02	00	other	autre
15944-5	02	01	seller is responsible	
15944-5	02	02	buyer is responsible	
15944-5	02	03	seller and buyer are both responsible	
15944-5	02	04	buyer shall specify to seller what IB to retain, (e.g., order number, transaction number, etc.)	
15944-5	02	05	seller and buyer shall use a common third party, (e.g., a notary)	
15944-5	02	06	regulator is responsible	
15944-5	02	07	regulator and seller are responsible	
15944-5	02	08	regulator and buyer are responsible	
15944-5	02	09	regulator, buyer and seller are all responsible	
15944-5	02	10	regulator mandates the involvement of a (role) qualified or designated third party, i.e., on behalf of seller, buyer and regulator.	
15944-5	02	98	not known	inconnu
15944-5	02	99	not applicable	sans objet

On the whole, the greater and more specific the external constraint governing the nature of the good, service or right being transacted the more extensive and specific the records retention requirements, (e.g., a learning transaction involving a professional (and regulated) qualification such as that for a medical doctor, an engineer, a lawyer, etc., requires records retention of a much more detailed nature than that for a general arts degree).

It is common external constraints of jurisdictional domains that a Person is required to retain sets of recorded information for a specified period of time. This is even more so where the recorded information pertains to a learning transaction (and particularly where the buyer is an individual).

[120)] NOTE Should there be a requirement for additional conditions for the specification of records retention responsibilities these can be added via a Technical Corrigenda to this standard or in the next edition of this standard.

External constraints of a records retention nature have requirements which specify (1) when a retention requirement is to start, i.e., via a limited number of triggers; and, (2) then a specified (minimum) retention period. On the whole, records retention requirements are triggered by an action or event. The basic conditions here from an external constraints perspective for "retention triggers" are limited. The most common ones are presented in the following Coded Domain 04 of ISO/IEC 15944-5.

Rule D-008:
Where an individual is an individual learner to a learning transaction, the LET provider shall specify the "retention trigger" activating records retention requirements in accordance with privacy protection requirements of the applicable jurisdictional domain(s).

Guideline D-008G1:
In support of Rule E-006, the LET provider as well as any other parties to the learning transaction, (e.g., a regulator, an agent, and/or third party) should use the ISO/IEC 15944-5 Coded Domain 04 "Codes representing retention triggers".

It is reproduced here below as Table D-4.

Table D.4 **— ISO/IEC 15944-5:04 Codes representing retention triggers**[121)]

ISO/IEC 15944-5:04 Codes Representing Retention Triggers				
IT Interface			**Human Interface Equivalent: Linguistic – Written Form**	
Source Authority ID	**Coded Domain ID**	**ID Code**	**ISO English**	**ISO French**
15944-5	04	00	other	autre
15944-5	04	01	start required retention period at date/time recorded information was received, created or collected	
15944-5	04	02	start required retention period from date of last action or use	
15944-5	04	03	start retention period at end of calendar year	
15944-5	04	04	start retention period at end of fiscal year	
15944-5	04	98	not known	inconnu
15944-5	04	99	not applicable [122)]	sans objet

[121)] NOTE Should there be a requirement for additional conditions for the specification of records retention responsibilities these can be added via a Technical Corrigenda to this standard or in the next edition of this standard.

[122)] This would apply to recorded information deemed to be ephemeral or transitory in nature and thus would (likely) also have an ID code of 99 under Coded Domain 15944-5:03.

D.4 Records Destruction

A key privacy protection requirement is that of the mandatory destruction, i.e. as the reverse of records retention. Within an information/records management and archiving context this is known as "disposition". Disposition is an authorized action to remove, i.e., alienate, a set of recorded information, from under the control of a Person and thereby extinguishing ownership and accountability[123)] In the context of this standard, “Open-edi disposition” is defined as:

> ***Open-edi disposition***
> ***process*** *governing the implementation of formally approved records retention, destruction (or expungement) or transfer of* ***recorded information*** *under the control of a* ***Person*** *which are documented in disposition authorities or similar instruments*
>
> *[adapted from ISO 15489-1:2001, 3.9]*

There are basically a limited number of disposal actions. These are identified in the following coded domain 03 found in ISO/IEC15944-8.

Rule D-009:
Where an individual participates in the role of an individual learner to a learning transaction, the LET provider shall specify the disposition action to be taken at the end of the expiry of the record retention period in accordance with privacy protection requirements of the applicable jurisdictional domain.

Guideline D-009G1:
In support of Rule D-007, the LET provider as well as any other parties to the learning transaction, (e.g., a regulator, an agent, and/or third party) should use the ISO/IEC 15944-5 Coded Domain 03 “Codes representing disposition of recorded information” as and where applicable.

Guideline D-009G2:
It is a recommended best practice for a LET provider to inform the individual learner that it by law or best practice will retain specified SRIs on the individual learner as long as that organization exists, (e.g., the fact that the individual learner “graduated” at whatever level of accomplishment).

It is reproduced here below as Table D.5.

[123)] This is more than “erasing” or “deleting” an SRI in an IT system. From an “evidentiary” requirements perspective, the requirement here is that of “expungement” (= eliminate completely, wipe out, destroy or obliterate an electronic record).

Table D.5 — ISO/IEC 15944-5:03 Codes representing disposition of recorded information[124)]

ISO/IEC 15944-5:03 Codes Representing Disposition of Recorded Information				
IT Interface			Human Interface Equivalent: Linguistic – Written Form	
Source Authority ID	Coded Domain ID	ID Code	ISO English	ISO French
15944-5	03	00	other	autre
15944-5	03	01	destruction or expungement	
15944-5	03	02	transfer to another organization	
15944-5	03	03	transfer to an archive (for historical and research purposes)	
15944-5	03	04	do not destroy, maintain and conserve as a permanent SRI	
15944-5	03	98	not known	inconnu
15944-5	03	99	not applicable [125)]	sans objet

[124)] NOTE Should there be a requirement for additional conditions for the specification of records retention responsibilities these can be added via a Technical Corrigenda to this standard or in the next edition of this standard.

[125)] This would apply to recorded information deemed to be transitory or ephemeral which can be discarded anytime.

[THIS PAGE IS INTENTIONALLY LEFT BLANK]

Annex E
(informative)

Use and adaptation of the ISO/IEC 14662 Open-edi Reference Model

E.1 Introduction

A very significant aspect of the ISO/IEC 14662 “Information technology -Open-edi Reference Model/ Technologies de l’information – Modèle de reference EDI-ouvert”, is that it focuses on the making of commitments among autonomous parties as a whole. ISO/IEC 14662 is very important in that (1) it is transaction-based; and, (2) that these transactions pertain to and support the making of commitments among Persons. Further the Open-edi Reference Model addresses the totality of standardisation requirements in support of learning transaction, and acknowledges that these need to be viewed from two different but complementary perspectives.[126)] The Open-edi Reference Model therefore makes a clear distinction between two perspectives; namely:

1) the Business Operational View (BOV); and,

2) the Functional Services View (FSV).

Figure E.1 below is a copy of Figure E.1 in ISO/IEC 14662

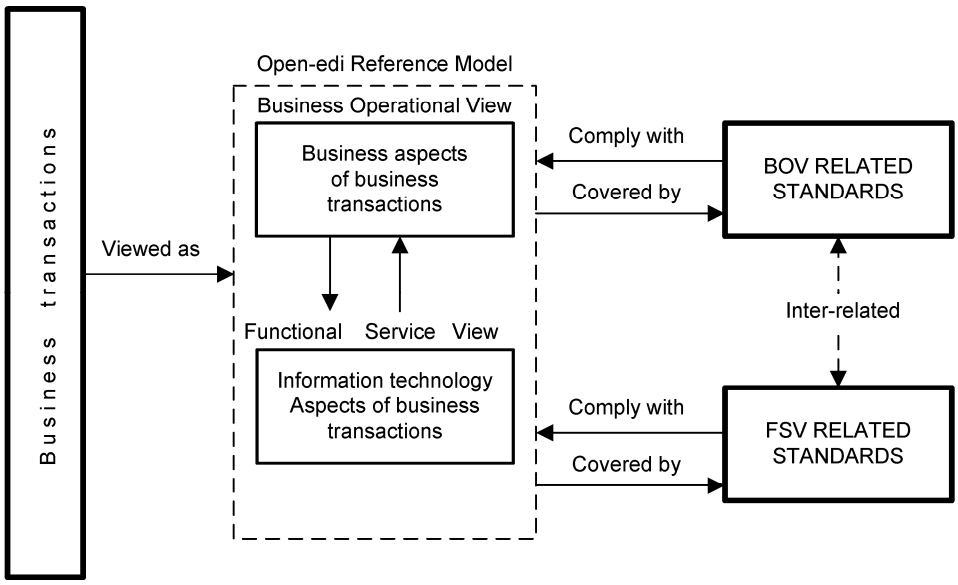

Figure E.1 — Open-edi environment – Open-edi Reference Model

[126)] The ISO/IEC 14662 Open-edi Reference Model serves as the basis of the 2000 Memorandum of Understanding (MOU) between ISO, IEC, ITU and the UN/ECE on concerning standardization in the field of electronic business (see< http://www.itu.int//ITU-T/e-business/files/mou.pdf >

E.2 Relevance of Open-edi Reference Model

Applying the Open-edi reference Model to this multipart ISO/IEC 29187 standard is and based on the premises that:

1) personal information is something of value;

2) the individual learner must give informed consent before its personal information can be collected and used by an organization or public administration;

3) there are rules governing the use, disclosure, retention, accuracy, safeguards, etc., that apply to personal information; and,

4) in fact, the organization or public administration is required by law to make a commitment to comply with privacy protection requirements.

As such, one can view privacy protection requirements as a form of commitment exchange imposed on organizations and public administrations with respect to the personal information of an individual learner.

In addition, the purpose and goal of the exchange of personal information between the individual learner and the organization must be stated and agreed to. Personal information collected for one purpose, i.e., as a mutually agreed to common goal, may not be used for another purpose without the individual's consent.

Therefore one can model these exchanges of personal information between the individual learner and a LET provider pertaining to a specified goal as "learning transactions" and apply the Open-edi Reference Model, illustrated in Figure E.2 as follows

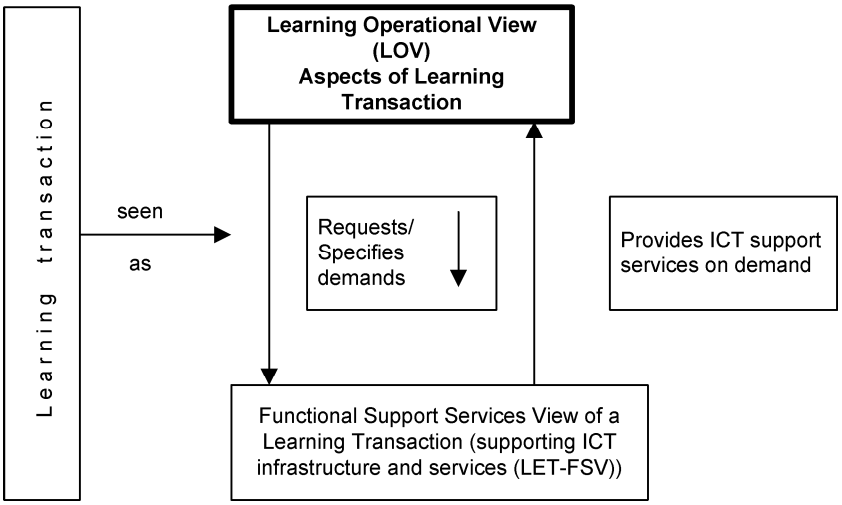

Figure E.2 — Learning transaction – Privacy Protection – Framework Model

The initial focus of the development of ISO/IEC 29187-1 will be on the development of the "Learning Operational View" aspects.

The draft working definition of "learning transaction" is;

> ***learning transaction***
> *predefined set of activities and/or **processes** among **Persons** which is initiated by a **Person**, i.e. in the role of **individual learner**, **LET provider** and/or **regulator**, involving the exchange of **recorded information**, to accomplish an explicitly stated learning goal and terminated upon recognition of one of the agreed conclusions by all the involved **Persons** although some of the recognition may be implicit*

NOTE 1 A learning transaction is realized through the exchange of verbal and recorded information and directed towards some mutually agreed upon goal extending over a period of time.

NOTE 2 A learning transaction may be internal constraints-based or external constraints-based. A primary example of an external constraint-based learning transaction is that of jurisdictional domains governing minimum levels of schooling, (e.g., K-12).

NOTE 3 A learning transaction can be on a for-a-fee or for-free basis.

NOTE 4 A LET provider can offer a learning transaction and operate on either a for-profit or not-for-profit basis.

NOTE 5 A learning transaction can consist of two or more learning transaction, each having their own stated (detailed) goal, yet at the same time forming part of a (overall goal).

[ISO/IEC 29187-1, 3.070]

The three key roles in a learning transaction are “buyer”, “seller” and “regulator”. In a learning transaction in a privacy protection environment, these would become “individual learner”, “LET provider” and regulator.

Figure E.3 below summarizes this approach. To this we have also added the “consumer protection” requirements environment

Figure E.3 — Summary of 3 key roles in a learning transaction

Environment	Role (in transaction	Role (in transaction)	Role (in transaction)
Generic	**user**	**supplier**	**(regulator)**
learning transaction (generic)	buyer	seller	regulator
learning transaction (Privacy protection)	individual learner	LET provider	regulator
consumer protection	consumer	vendor	regulator

ISO/IEC 2382-36:2009 *“Information technology — Vocabulary — Part 36: Learning, Education, and Training / Technologie de l’information — Vocabulaire — Partie: Apprentissage, education et formation” defines “learner” as:*

learner
entity that learns

apprenant
entité qui apprend
[ISO/IEC 2382-36, 36.02.01]

Since privacy protection requirements do not apply to any kind of entity but only to individuals, the concept and definition of “individual learner” is being introduced with the following draft definition:

individual learner
*learner who participates as an **individual** in a **learning transaction***

[ISO/IEC 29187-1, 3.055]

Similarly, within a LET environment, the use of “seller” & “vendor” are not that favoured. In any case these concepts and their terms are already “taken” and it is important to have a distinct concept, definition and associated term for use in a LET environment. Thus we have the following draft working definition:

> ***LET provider***
> ***Person,*** *as* ***organization*** *or* ***public administration*** *which provides a good, service, and/or right in the fields of learning, education or training as part of a* ***learning transaction***
>
> *[ISO/IEC 29187-1, 3.079]*

Here one notes that the role of “regulator” and its definition is essentially generic in nature and applies in any environment or sector. Amending the existing definition for “regulator / autorité de réglementation” and substituting provides the following definition for this concept.

The focus of the Open-edi and eBusiness standards is that of modelling the collaboration space among the primary parties to a learning transaction. For modelling purposes, a learning transaction requires at the least the roles of a “buyer” and a “seller,” based on “internal constraints” only. Depending on the nature of the LET good, service and/or right (or combination of the same) one or more sets of “external constraints” may apply. These are modelled through the introduction of the role of a “regulator”.

This section summarizes “collaboration space” as already defined along with applicable rules in Parts 4 and 5 of ISO/IEC 15944 and does do from a Part 8 from a Privacy Protection requirements perspective.

E.3 Basic aspects of Open-edi collaboration space: Buyer and seller

The primary purpose of collaboration space is to avoid having the same commitment exchanges comprising a learning transaction from being modelled multiple times, i.e., as mirror images views of the same sets of recorded information being interchanged among “Persons” in their roles of “buyer” and “seller” as information bundles (IBs) (and their semantic components (SCs)), as part of the scenario governing a learning transaction. By way of example, the “receipt of a sale” between a buyer and seller contains exactly the same information with respect to:

1) the learning transaction identifier (BTI);

2) date (and time) of sale, i.e., the date of the instantiated learning transaction;

3) the price paid (often before and then including applicable taxes);

4) identification (at various levels of granularity) of what was purchased/sold

5) the means and mode of payment;

6) conditions, warranties, rebates, etc., as applicable; and,

7) any other documentation provided (including that as part of the packaging, recorded information in the packaging, or “online” via the Internet, including where it is a “virtual” LET good, service and/or right being transacted).

The purpose of business process modelling in the Open-edi context is to model the recorded information exchanged among the two primary Persons to a learning transaction. In that context there are two roles of Person, one assuming the role of “buyer” and the other the role of “seller”, and the focus is on the information bundles that are being interchanged among these two primary partners in the learning transaction.

From an Open-edi perspective, the collaboration space is a view of transactions that take place outside the internal control space of the Persons which are parties to a learning transaction. This view sees both interchanges of information, i.e., from seller to buyer and buyer to seller as conceptually similar. Such a perspective is quite different than that of the view taken from inside of an organization.

For Open-edi collaboration modelling, internal processes are not relevant until a resource as an information flow (or represented by it via a reference tag) crosses an organization's logical boundaries. This independent perspective is the focus of Open-edi and is represented by collaboration space where values in the form of sets of recorded information (SRIs) are interchanged among the parties to a learning transaction.

This is illustrated in Figure E.4 below (taken from Figure E.4 "Concept of a Business Collaboration" in ISO/IEC 15944-4:2007).

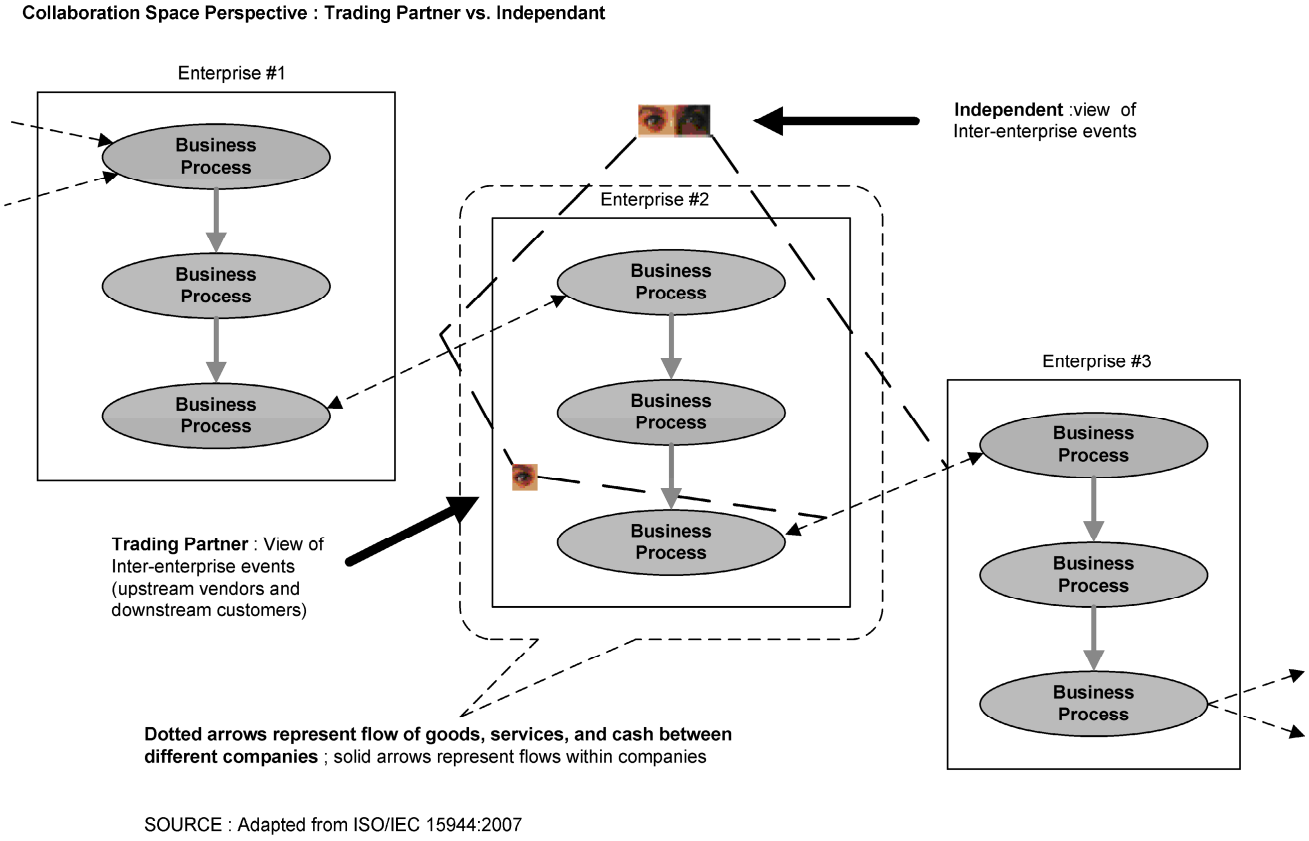

Figure E.4 —Concept of a Business Collaboration

The key and distinguishing aspect of the concept of collaboration space is that of providing an "independent view" from that of the specific views of each of the parties to a commitment exchange. In the ISO/IEC 15944-4 standard which focuses on "accounting and economic ontology" the parties to the collaboration space in support of the establishment of a commitment exchange, instantiated as a transaction, are "trading partners" and the application field is that of a "business transaction".

In this ISO/IEC 29187-1 Framework and Reference Model which focuses on a learning, education, and training (LET) context, the (primary) parties to the collaboration space in support of the establishment of a commitment exchange, is instantiated as a transaction, are the individual learner and the LET provider and the application field is that of a "learning transaction".

[THIS PAGE IS INTENTIONALLY LEFT BLANK]

Annex F
(informative)

Potential parts 2+ for ISO/IEC 29187 based on results of the ISO/IEC JTC1/SC 36 Ad-Hoc on Privacy (AHP)

F.1 Introduction

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[127)] 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.[128)] 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[129)]

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. Additional contributions to the AHP provided additional 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. 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-member must be able, or structured to be able, to support applicable privacy protection requirements.

F.2 Purpose

The purpose of this Annex F is to present, in summary form, the privacy protection issues to be addressed in an ITLET context in Parts 2+ of ISO/IEC 29187 based on the integration of the results of the:

a) work of the ISO/IEC JTC1/SC36 AHP; and,

b) P-member ballot comments of the development of this Part 1.

In addition, it is noted that it may well be that some of the issues listed below, and already identified by JTC1/SC36 P-members as requiring the development of Parts 2+ can be combined into the development of one or more discrete and focused Parts 2+ of ISO/IEC 29187.

---

127) 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.

128) These privacy/data protection related standards development projects have been identified by the JTC1/SC36 Ad-Hoc on Privacy and are summarized in the ISO/IEC JTC1/SC36 N1737 NWIP for this multipart standard.

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

F.3 User requirements and issues identified by the SC36/AHP of sub-types of data in a LET context requiring privacy protection standard(s)[130)]

The user requirements and issues identified by JTC1/SC36 P-members as a result of the work of the SC36 AHP with respect to its "survey Question 4 – Identification of types of data in a LET context requiring privacy protection 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.)[131)]
- any information pertaining to work experience;
- 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;
- that of post-secondary institutions, as per their internal guidelines;
- all ITLET 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 protection requirements to electronic data interchange among autonomous parties with respect to personal information of a "LET" nature.

[130)] Based on Annex E.2 in 36N1737

[131)] Note: There is a link here to the JTC1/SC36 standards development work on the multipart ISO/IEC 24751 and 20016 standards.

F.4 User requirements of specific LET needs pertaining to privacy issues[132)]

LET 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[133)]
- 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 MySpace, Facebook, wikis, You Tube, blogs, etc.). Here "best practices" in ITLET need to be more broadly promoted and implemented. These and related pedagogical issues could perhaps be supported by appropriate standards.

F.5 User requirements for ISO/IEC 29187-1 resulting from JTC1/SC36 resolution

The SC36 N1737 NWIP document adopted in 2009 cites JTC/SC36 Resolution 19: (Stuttgart 2008): Privacy issues. It reads as follows:

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

a) access to mobile information, and in particular access to contextual information;

b) identifying information related to e-portfolios;

c) applications of sensor technologies to LET, and in particular, applications to assessments, learner localization, etc.

This list may not be exhaustive.

F.6 User requirements for Parts 2+ resulting from responses to JTC1/SC36/WG3 N360

It is noted that privacy protection requirements applicable to a learning transaction involving an individual learner and a LET provider have in their implementation requirements need to ensure the accuracy, integrity, and trustworthiness of all the recorded information with respect to:

1) all aspects of knowledge certifications which an operation of evaluation which results in (a) progress; and, (b) results of any individual learner in a learning transaction as personal data which may require additional and more specific privacy protection requirements;

[132)] Based on Annex E.3 in 36N1737

[133)] 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).

2) addressing privacy protection requirements which may be common to a specified group of individual learners as refined by a pedagogic category, (e.g., a class, group, team, etc.) including:

   a) a specific privacy protection protocol which is applied to such a pedagogic category;

   b) the specific results of the application of the same; and,

   c) the specific result of the application of 2a) and 2b) to an individual learner.

3) a final evaluation of the result of any individual learner which could apply (generally) to:

   a) quantitative elements as a result(s) in a given test, to a set of exams, to any applied task occurring in the framework of the delivery of a tracking sequence;

   b) quantitative appreciation which take the final form of a given certification, diploma, etc., which, as a whole, are more than the quantitative result of an ITLET process (and refers to a global aptitude guaranteed by the teaching body.

4) identifying and addressing possible added privacy protection requirements pertaining to a “collective learner” (multi-peer) where the learning transaction involves the participation of two or more individual learners in a “collection”. {See Figure F.3 above}

5) addressing possible added privacy protection requirements pertaining to a LET provider “consortium” where two or more Let providers are involved in a learning transaction with an individual learner. An example is where two (at times three) LET providers jointly offer a degree, diploma, certificate, etc., programme. There is the need to ensure that privacy protection requirements apply[134)]

[134)] An increasing number of university degree programs include, the offering or requirement for the individual learner to participate in a “stage”, a one-month study, etc., at a LET provider other than which the individual learner is enrolled. On the whole these other LET providers are in jurisdictional domains other than that of the individual learner and/or that of the LET provider in which the individual learner is enrolled.

Bibliography

This bibliography is organized in two parts. The first identifies sources that are ISO and ISO/IEC international standards. The second cites other cited sources which are useful to the understanding of this part of ISO/IEC 9187.

1) ISO and ISO/IEC international standards

ISO/IEC 9798-1:1997 (E), *Information technology — Security techniques — Entity authentication — Part 1: General.*

ISO/IEC 10181-2:1996, *Information technology — Open System, Interconnection — Security frameworks for open systems — Part 2: Authentication framework.*

ISO/IEC 11179-1:2004 (E), *Information technology — Metadata registries (MDR) — Part 1: Framework.*

ISO/IEC 11179-3:2003 (E), *Information technology — Metadata Registries (MDR) — Part 3: Registry Metamodel and basic attributes.*

ISO/IEC 14662:2009 (E/F*)*, *Information technology — Open-edi Reference Model/Technologies de l'information — Modèle de référence EDI-ouvert.*

ISO/IEC TR 15285:1998 (E), *Information technology — An operational model for characters and glyphs*.

ISO/IEC 15944-6:2008 (E), *Information technology — Business Operational View — Part 6: Technical Introduction of eBusiness modelling*.

ISO 19135:2005 (E), *Geographic information — Procedures for registration of items of geographic information*.

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management.*

2) Other

36N1737, *"New Work Item (NP) on Information technology — Identification of Privacy Protection requirements pertaining to learning, education and training (LET)".*

Quittner, Joshua. (Monday, 8 February, 1999). Going private. Time 153(5):62 (8 February, 1999). Retrieved 18 November, 2010 from http://www.time.com/time/magazine/article/0,9171,990168,00.html.

UN. International Covenant on Economic, Social and Cultural Rights 1966. Retrieved 18 November, 2010 from http://www2.ohchr.org/english/law/cescr.htm.

UN. Universal Declaration of Cultural Diversity (Paris, November, 2001) Retrieved 18 November, 2010 from http://www2.ohchr.org/english/law/diversity.htm.

UN. Universal Declaration of Human Rights (1948) Retrieved 18 November, 2010 from http://www.un.org/en/documents/udhr/.

UN. Universal Declaration of Rights of Persons belonging to National or Ethnic, Religious and Linguistic Minorities" (15 December, 1992). Retrieved 18 November, 2010 from: http://www2.ohchr.org/english/law/minorities.htm.

ICS 03.100.30; 35.240.99

Price based on 174 pages