INTERNATIONAL STANDARD

ISO/IEC 15944-12

First edition
2020-05

Information technology — Business operational view —

Part 12: Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information (PI)

Technologies de l'information — Vue opérationnelle d'affaires —

Partie 12: Exigences en matière de protection de la vie privée (PPR) relatives à la gestion du cycle de vie de l'information (ILCM) et de l'EDI des renseignements personnels (PI)

Reference number
ISO/IEC 15944-12:2020(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 32, *Data management and interchange*.

A list of all parts in the ISO/IEC 15944 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

NOTE This document is intended to be used in conjunction with ISO/IEC 14662, ISO/IEC 15944-1, ISO/IEC 15944-5 and ISO/IEC 15944-8.

0.1 Purpose and overview

Modelling business transactions using scenarios and scenario components includes specifying the applicable constraints on the data content using explicitly stated rules. ISO/IEC 14662 identifies two basic classes of constraints, "internal constraints" and "external constraints". External constraints apply to most business transactions. External constraints have governance over any processing of personal information including that exchanged among parties to a business transaction and doing so from an information life cycle management (ILCM) requirements perspective.

Jurisdictional domains are the primary source of external constraints on business transactions (see Annex C). Privacy protection requirements in turn are a common requirement of most jurisdictional domains, although they may also result from explicit scenario demands from or on the parties involved in a business transaction. (Requirements for secrecy or confidentiality are not addressed in this document, unless they are implicitly needed to apply privacy protection requirements to data).

The focus of this document is on any kind of recorded information concerning identifiable living individuals as buyers in a business transaction or whose personal information is used in a business transaction or any type of commitment exchange.

This document describes the added business semantic descriptive techniques needed to support information life cycle management (ILCM) aspects as part of privacy protection requirements when modelling business transactions using the external constraints of jurisdictional domains. ILCM aspects are central to the ability to ensure that privacy protection requirements (PPR) are passed on and supported among all the parties to a business transaction using EDI.

This document applies to any organization which receives, creates, process, maintains, communicates, etc. personal information (PI) and, in particular, to those who receive, create, capture, maintain, use, store or dispose of sets of recorded information (SRIs) electronically. This document applies to private and public sector activities of Persons irrespective of whether such activities are undertaken on a for-profit or not-for-profit basis.

This document is intended for use by those organizations to which privacy protection requirements apply and who therefore need to ensure that the recorded information (electronic records and transactions) in their IT Systems is trustworthy, reliable and recognized as authentic. Typical users of this document include

a) managers of private and public sector organizations;

b) IT systems and records/information management system professionals;

c) privacy protection officers (PPOs) and other personnel in organizations, including those responsible for risk management; and

d) legal professionals and others within an organization responsible for information law compliance by the organization.

0.2 Use of ISO/IEC 14662 and ISO/IEC 15944

0.2.1 ISO/IEC 14662: Open-edi reference model[1)]

ISO/IEC 14662[2)] states the conceptual architecture necessary for carrying out electronic business transactions among autonomous parties. That architecture identifies and describes the need to have two separate and related views of the business transaction.

The first is the business operational view (BOV). The second is the functional service view (FSV). Figure 1, taken from ISO/IEC 14662:2010, Figure 1, illustrates the Open-edi environment. (For definitions of the terms used, see Clause 3.)

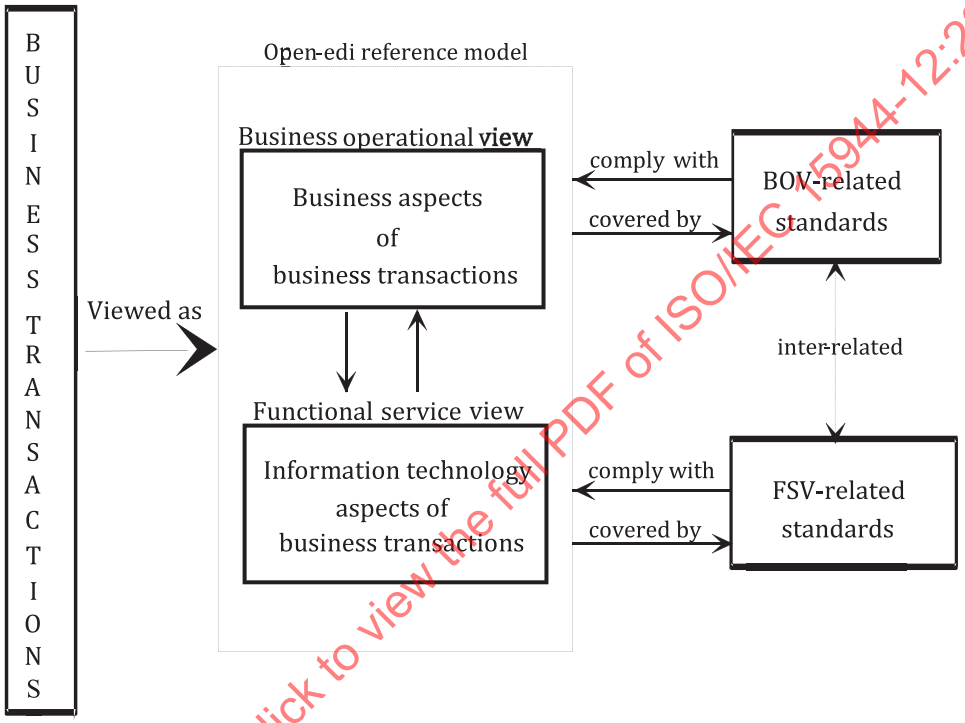

Figure 1 — Open-edi reference model environment

ISO/IEC 15944 is a multipart eBusiness standard which is based on and focuses on the BOV perspective of the ISO/IEC 14662 Open-edi reference model. This document focuses on addressing commonly definable aspects of external constraints that relate to information life cycle management (ILCM) in a privacy and data protection[3)] context when the source is a jurisdictional domain. A useful characteristic of external constraints is that, at the sectoral level, national and international levels, etc., focal points and recognized authorities often already exist. The rules and common business practices in many sectoral areas are already known. Use of this document (and related standards) addresses the transformation of these external constraints (business rules) into specified, registered, and re-useable scenarios and scenario components.

1) The Memorandum of Understanding between ISO, IEC, ITU and UN/ECE (2000) concerning standardization in the field of electronic business is based on this *Model*. See https://www.unece.org/fileadmin/DAM/oes/MOU/2000/24March2000_IEC_ISO_ITU.pdf.

2) ISO/IEC 14662 is freely-available at https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

3) "Privacy protection" is the common set of worldwide requirements. In the European Union, "data protection" is the equivalent concept (used mainly due to historical reasons). In many other non-European countries,(Australia, Canada, New Zealand, USA, etc., "privacy" is the legal term used in applicable legislation and pursuant regulations. This is because "privacy" applies to not just "data" but any form of recorded information containing "personal information". Thus from an international standards perspective "privacy protection" integrates "privacy" and "data protection" requirements. In many other countries, "privacy" is the legal term used in applicable legislation and pursuant regulations.

This document is based on ISO/IEC 14662 as well as existing parts of the ISO/IEC 15944 series, which serve as its key normative references and overall boundaries for the scope of this document. ISO/IEC 15944-5 and ISO/IEC 15944-8, in particular, serve as the basis for this document as they both focus on external constraints.

0.2.2 ISO/IEC 15944-1: Business operational view (BOV) – operational aspects of Open-edi for implementation

ISO/IEC 15944-1 states the requirements of the BOV aspects of Open-edi in support of electronic business transactions. They are required to be taken into account in the development of business semantic descriptive techniques for modelling e-business transactions and components thereof as re-useable business objects. They include:

— Commercial frameworks and associated requirements.

— Legal frameworks and associated requirements.

— Public policy requirements particularly which apply to individuals, i.e., are rights of individuals, which are of a generic nature such as consumer protection, privacy protection, and accessibility (see ISO/IEC 15944-5:2008, 6.3).

— Requirements arising from the need to support cultural adaptability. This includes meeting localization and multilingual requirements, (e.g., as can be required by a particular jurisdictional domain or desired to provide a good, service and/or right in a particular market). Here one needs the ability to distinguish, the specification of scenarios, scenario components, and their semantics, in the context of making commitments, between:

  a) the use of unique, unambiguous and linguistically neutral identifiers (often as composite identifiers) at the information technology interface level among the IT systems of participation parties on the one hand; and, on the other,

  b) their multiple human interface equivalent (HIE) expressions in a presentation form appropriate to the Persons involved in the making of the resulting commitments.

Figure 2, based on ISO/IEC 15944-1:2011, Figure 3, shows an integrated view of these business operational requirements. Since the focus of this document is that of external constraints for which jurisdictional domains are the primary source, these primary sources have been shaded in Figure 2.

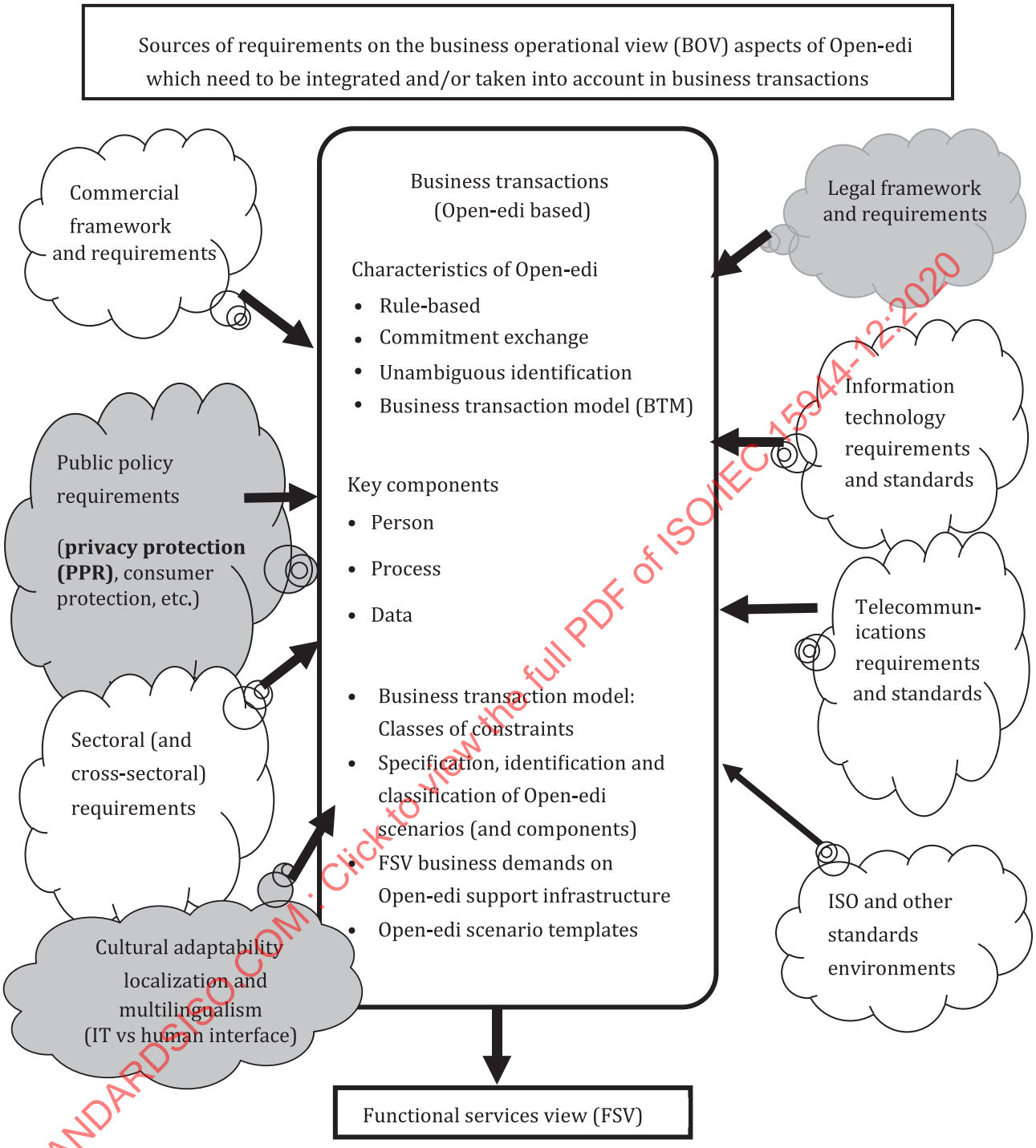

Figure 2 — Integrated view of business operational requirements with an external constraints focus

In electronic business transactions, whether undertaken on a for profit or not-for-profit basis, the key element is commitment exchange among Persons made through their decision-making applications (DMAs) of their information technology systems (IT Systems, see ISO/IEC 14662:2010, 5.2) acting on behalf of "Persons". "Persons" are the only entities able to make commitments.

The **business operational view (BOV)** was defined as:

*"perspective of **business transactions** limited to those aspects regarding the making of **business** decisions and **commitments** among **Persons** which are needed for the description of a **business transaction**".*

[SOURCE: ISO/IEC 14662:2010, 3.3]

There are three categories of Person as a role player in Open-edi, namely: (1) the Person as "individual", (2) the Person as "organization", and (3) the Person as "public administration"[4]. There are also three basic (or primitive) roles of Persons in business transactions, namely: "buyer", "seller", and "regulator". When modelling business transactions, jurisdictional domains prescribe their external constraints in the role of "regulator" and execute them as "public administration".

0.2.3 Link to ISO/IEC 15944-5 and ISO/IEC 15944-8

ISO/IEC 15944-5 focuses on external constraints the primary source of which is jurisdictional domains, at various levels. It also identified a common class of external constraints known as "public policy", which apply where and when the "buyer" in a business transaction is an "individual". It identified three key sub-types, along with applicable rules; of public policy constraints, namely "consumer protection", "privacy protection" and "individual accessibility" (see ISO/IEC 15944-5:2008, 6.3). In addition, ISO/IEC 15944-5 specifies how and where (common) external constraints of jurisdictional domains impact the "Person", "process", and "data "components of the business transaction model (BTM), as introduced in ISO/IEC 15944-1.

ISO/IEC 15944-8, which is based on ISO/IEC 15944-5, focuses on providing a more detailed identification and specification of the common privacy protection requirements as they apply to any business transaction where the buyer is an individual.

This document:

— is based on both ISO/IEC 15944-5 and ISO/IEC 15944-8;

— integrates applicable concepts and definitions, principles, rules, etc., found in both ISO/IEC 15944-5 and ISO/IEC 15944-8 (as well as applicable elements of the Open-edi reference model and other parts of the ISO/IEC 15944 series); and

— focuses on information life cycle management (ILCM) aspects at a more granular level, i.e., that required to be able to support implementation of the same.

0.3 Link to Privacy-by-Design (PbD) [48] approach

The overall purpose of the Privacy by Design (PbD) approach is to ensure that privacy protection requirements (as stated in applicable legal and/or regulatory requirements) are identified and specified in a systematic and rule-based manner for those developing any IT systems within their organization.

It is noted that although this is the first part in the ISO/IEC 15944 series in which Privacy by Design is formally mentioned, the PbD approach has always been supported and "imbedded" in the development of the ISO/IEC 15944 series. The need to comply with and support privacy protection requirements was already incorporated in ISO/IEC 15944-1:2002, D.1.1.

The development of the ISO/IEC 15944 series fully supports the seven "foundation principles" of the PbD approach[5]. In particular it provides the detailed rules, definitions and related guidelines necessary

4) While "public administration" is one of the three distinct sub-types of Person, most of the rules in this document applicable to "organization" also apply to "public administration". In addition, an unincorporated seller is also deemed to function as an "organization". Consequently, the use of "organization" throughout this document also covers "public administration". Where it is necessary to bring forward specific rules, constraints, properties, etc., which apply specifically to "public administration", this is stated explicitly.

5) 1. Proactive and not reactive; preventative and not reactive; 2. Privacy as the default setting; 3. Privacy embedded in design; 4. Full functionality – positive-sum, not zero-sum; 5. End to end security – full lifecycle protection; 6. Visibility and transparency – keep it open; 7. Respect for user privacy – keep it user-centric. [48]

to ensure that privacy protection requirements are identified and implemented not only throughout the entire life cycle of the recorded information involved, i.e., "cradle-to-grave", information life cycle management (ILCM) but especially that for any personal information interchanged via EDI among parities to a particular business transaction.

0.4 Importance and role of terms and definitions

The ISO/IEC 15944 series sets out the processes for achieving a common understanding of the business operational view (BOV) from commercial, legal, ICT, public policy and cross-sectoral perspectives. It is therefore important to check and confirm that a "common understanding" in any one of these domains is also unambiguously understood as identical in the others.

This subclause is included in each part of the ISO/IEC 15944 series to emphasize that harmonized concepts and definitions (and assigned terms) are essential to the continuity of the overall series.

In order to minimize ambiguity in the definitions and their associated terms, each definition and its associated term has been made available in at least one language other than English in the document in which it is introduced. In this context, it is noted that ISO/IEC 15944-7 already also contains human interface equivalents (HIEs) in ISO Chinese, ISO French, and ISO Russian[6)]

0.5 Based on rules and guidelines

This document is intended to be used by diverse sets of users having different perspectives and needs (see Figure 2).

The ISO/IEC 15944 series focuses on "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".

Open-edi is based on rules which are predefined and mutually agreed to. They are precise criteria and agreed-upon requirements of business transactions representing common business operational practices and functional requirements.

These rules also serve as a common understanding bridging the varied perspectives of the commercial framework, the legal framework, the information technology framework, standardisers, consumers, etc.[7)]

0.6 Use of "Person", "organization", "individual" and "party" in the context of business transaction and commitment exchange

Throughout this document:

— the use of Person with a capital "P" represents Person as a defined term, i.e., as the entity within an Open-edi Party that carries the legal responsibility for making commitment(s);

— "individual", "organization", and "public administration" are defined terms representing the three common sub-types of "Person"; and

— the use of the words "person(s)" and "party (ies)" without a capital "P" indicates their use in a generic context independent of "Person", as a defined concept in ISO/IEC 14662 and the ISO/IEC 15944 series.

NOTE A "party" to a business transaction has the properties and behaviours of a "Person".

6) The designation ISO before a natural language refers to the use of that natural language in ISO standards.

7) The working principle is that of "coordinated autonomy", i.e., all parties are autonomous. Therefore, the extent to which they cooperate, agree on common needs, business rules constraints, practices, etc., and reach agreement on the same in form of precise rules, terms and definitions, etc., is a key influence on the creation of necessary standards as well as common scenarios, scenario attributes and scenario components.

0.7 Use of "identifier" (in a business transaction) and roles of an individual

ISO/IEC 15944-1:2011, 6.1.4 focuses on the requirement for the unambiguous identification of entities in business transactions (see also ISO/IEC 15944-1:2011, Annex C). "Unambiguous" is a key issue in business transactions because states of ambiguity and uncertainty are an anathema from commercial, legal, consumer and information technology perspectives. Issues of unambiguousness apply to all aspects of a business transaction and even more so to those which are EDI-based. Open-edi transactions anticipate that all entities are fully and clearly identified prior to the instantiation of a business transaction.

0.8 Use of "jurisdictional domain" in the context of privacy protection and related ILCM requirements

The term "jurisdiction" has many possible definitions. Some definitions of "jurisdiction" have accepted international legal status while others do not. It is also common practice to equate "jurisdiction" with "country", although the two are by no means synonymous. It is also common practice to refer to states, provinces, länder, cantons, territories, municipalities, etc., as "jurisdictions", and in contract law it is customary to specify a particular court of law as having jurisdiction or a defined national body, or an international body as having jurisdiction (even if that is not legally enforceable), and so on. Finally, there are differing "legal" definitions of "jurisdiction". Readers should understand that in this document:

— the use of the term "jurisdictional domain" represents its use as a defined term; and

— the use of the terms "jurisdiction(s)" and/or "country (ies)" represents their use in their generic contexts and do not imply any legal effect per se.

0.9 Use of "privacy protection" in the context of business transaction, EDI and any type of commitment exchange

Jurisdictional domains, such as UN member states (and/or their administrative sub-divisions), have enacted various "privacy" laws, "data protection" laws, "protection of personal information" laws, etc. (as well as pursuant regulations). Some of these sources of legal requirements focus on the protection of personal information in IT systems only (e.g., "data protection"), while others focus on the protection of personal information irrespective of the medium (see ISO/IEC 15944-1:2011, 6.4.1) used for the recording of personal information and/or its communication to other Persons.

In the case of personal information, this is currently defined by most jurisdictional domains to be a specific sub-set of recorded information relating to the Person as an "individual" — where the qualities of such type of Person are that they are required to be an identifiable, living individual. As a consequence, this may only apply to some proportion of the specific role players in a business transaction (including their personae) and not others.

The delivery of "privacy protection" requires action both at the business operational level (BOV) and functional services view (FSV) (or technology levels). Where human beings interact with recorded information once it has passed through an Open-edi transaction, they have the potential to compromise technical controls (FSV) that could have been applied. It is essential that business models take into account the need to establish overarching business 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 protection demands of regulation that are required to be applied to personal data, their use, prescribed dissemination and so on. In this regard, the interplay of the BOV and FSV views of all organizations is important.

0.10 Use of "set of recorded information" (SRI) and "set of personal information" (SPI) versus record, document, message, data, etc.

The concepts of "record", "document", "data", "message", etc., are defined and used in ISO standards and in different levels of jurisdictional domains. However, multiple differing definitions exist for each of these terms. To address this polysemy issue, the unifying concept and definition of "set of recorded information" was introduced and defined in ISO/IEC 15944-5.

In Open-edi, SRIs are modelled as information bundles (IBs) and semantic components (SCs) when they are interchanged among participating parties in a business transaction. Within the IT systems of an organization, and especially within its decision-making applications (DMAs), the recorded information pertaining to a business transaction is usually maintained as one or more (linked) SRIs.

In order to maximize linkages between Open-edi (external behaviour) aspects and data management (internal behaviour) aspects of an organization (as well as associated record management and EDIFACT standards), SRI is used as a common higher level concept, which incorporates essential attributes of the concepts of "record", "document", "message", etc. as defined in various ways in existing ISO standards.

Where and when a SRI is of the nature of personal information or contains personal information, privacy protection requirements (PPR) apply. Within the context of PPR and with the focus of ILCM the concept and definition of "*set of personal information (SPI)*" is as follows:

— ***set of personal information (SPI)***;

— ***set of recorded information (SRI)*** *which is of the nature of or contains* ***personal information***.

This document focuses on ILCM of personal information in support of PPR and as such *"set of personal information (SPI)"* is used throughout this document while *"set of recorded information* (SRI) when referring to the more generic ILCM aspects.

0.11 Aspects currently not addressed

This first edition of this document focuses on the essential and basic ILCM aspects of privacy protection requirements.

Many other aspects identified in the development of this document remain to be addressed. For detailed information on these see Annex I.

0.12 IT-systems environment neutrality

This document, like all the other parts of ISO/IEC 15944, 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 document maximizes an IT-enabled approach to its implementation and maximizes semantic interoperability.

0.13 Organization and description of this document

This document identifies basic common requirements of information life cycle management (LCM) requirements in a privacy protection context, as external constraints of jurisdictional domains, on the modelling of a business transaction through scenarios and scenario components.

Following Clauses 0, 1, 2, 3 and 4, which have a common approach and similar content in the ISO/IEC 15944 series, Clause 5 summarizes the 11 "Fundamental privacy protection principles" introduced and defined in detail in ISO/IEC 15944-8:2012, Clause 5 along with its associated rules and guidelines. Clause 5 also provides a link to related "consumer protection" and "individual accessibility" requirements. A key purpose of Clause 5 is to place privacy protection principles in the content of ILCM requirements. A related purpose is to bring forward the requirement that any and all sets of personal information (SPIs) are identified, i.e., tagged or labelled, as such in support of privacy protection requirements.

Clause 6 identifies an integrated (minimum) set of ILCM principles along with associated rules and guidelines required to support both general information law requirements and in particular those required to be implemented in support of privacy protection requirements.

Clause 7 focuses on the need to ensure accountability for and control of personal information by any organization (or public administration). Clause 8 expands on this by providing the rules governing specification of ILCM aspects of personal information, i.e., from an implementation perspective.

The fact that in their "normal" operations organizations need to undertake data conversions and data migration in the decision-making applications (DMAs) of their IT systems is recognized in Clause 9. However, it is also important that applicable privacy protection requirements remain being supported, i.e., within and among, organizations including data synchronization among their IT systems.

Clause 10 summarizes key rules and requirements found in ISO/IEC 15944-1, ISO/IEC 15944-5 and ISO/IEC 15944-8 which govern EDI of personal information between the primary ILCM Person, i.e., seller, and its use of agents and/or third parties. The clause concludes with a conformance statement.

Finally, annexes are provided for elaboration of points raised in the main body. Of these Annexes A and B are normative, and the remaining annexes are informative.

Annex A is a consolidated list of the definitions and their associated terms introduced in this document in ISO English and ISO French. (For the complete set of ISO French (and ISO Russian and ISO Chinese) equivalents of the entries in Clause 3, see ISO/IEC 15944-7.) As stated in the main body of this document, the issue of semantics and their importance of identifying the correct interpretation across official aspects is critical.

Annex B identifies rules stated in the other parts of ISO/IEC 15944 that are applicable to this document.

Annex C is common to ISO/IEC 15944-2, ISO/IEC 15944-4, ISO/IEC 15944-5 and ISO/IEC 15944-8. It summarizes the business transaction model (BTM).

The focus of Annex D is to link the ILCM process to the process phases of a business transaction. Annex E provides a generic approach to ILCM decisions in a privacy protection requirements context along with an ILCM compliance decision tree template.

The purpose of Annex F is to provide a generic approach to the identification of properties and behaviours of PI as SRI transitory records and their disposition/expungement. In Annex G some notes on referential integrity in Open-edi are presented.

Annex H provides details on a number of exclusions to the scope of this document while Annex I identifies aspects of the scope of this document which have not yet been addressed in this current edition.

Annex J provides the list of all parts in the ISO/IEC 15944 series. Annex K contains abstracts in ISO English, French and Chinese.

Information technology — Business operational view —

Part 12: Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information (PI)

1 Scope

This document:

— provides method(s) for identifying, in Open-edi modelling technologies and development of scenarios, the additional requirements in business operational view (BOV) specifications for identifying the additional external constraints to be applied to recorded information in business transactions relating to personal information of an individual, as required by legal and regulatory requirements of applicable jurisdictional domains;

— integrates existing normative elements in support of privacy and data protection requirements as are already identified in ISO/IEC 14662 and ISO/IEC 15944-1, ISO/IEC 15944-2, ISO/IEC 15944-4, ISO/IEC 15944-5, ISO/IEC 15944-8, ISO/IEC 15944-9, and ISO/IEC 15944-10;

— provides overarching, operational 'best practice' statements for associated (and not necessarily automated) processes, procedures, practices and governance requirements that act in support of implementing and enforcing technical mechanisms which support the privacy/data protection requirements necessary for implementation in Open-edi transaction environments;

— focuses on the life cycle management of personal information i.e., the contents of SPIs (and their SRIs) related to the business transaction interchanged via EDI as information bundles and their associated semantic components among the parties to a business transaction.

NOTE Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information as stated in this document serve as a minimum set of ILCM policy and operational requirements for all recorded information pertaining to a business transaction in particular, as well as ILCM implementation in any organization in general.

This document does not specify the technical mechanisms, i.e., functional support services (FSV) which are required to support BOV-identified requirements. Detailed exclusions to the scope of this document are provided in Annex H.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitute requirements 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.

ISO/IEC 14662:2010, *Information technology — Open-edi reference model*

ISO/IEC 15944-1:—,[8] *Information technology — Business operational view — Part 1: Operational aspects of Open-edi for implementation*

ISO/IEC 15944-5:2008, *Information technology — Business operational view — Part 5: Identification and referencing of requirements of jurisdictional domains as sources external constraints*

8) Third edition under preparation. Stage at time of publication: ISO/IEC DIS 15944-1.

ISO/IEC 15944-8:2012, *Information technology — Business operational view — Part 8: Identification of privacy protection requirements as external constraints on business transactions*

3 Terms and definitions

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

For the human interface equivalents (HIEs) of each term in Clause 3 in ISO French, Annex A applies.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
address
set of *data elements* (3.32) that specifies a *location* (3.67) to which a *recorded information* (3.110) item(s), a *business object(s)* (3.8), a material *object(s)* (3.73) and/or a person(s) can be sent or from which it can be received

Note 1 to entry: An address can be specified as either a physical address and/or electronic address.

Note 2 to entry: 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 to entry: 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).

[SOURCE: ISO/IEC 15944-2:2015, 3.1]

3.2
agent
Person (3.89) acting for another *Person* in a clearly specified capacity in the context of a *business transaction* (3.10)

Note 1 to entry: Excluded 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)".

[SOURCE: ISO/IEC 15944-1:— 3.1]

3.3
anonymization
process (3.100) whereby the association between a *set of recorded information (SRI)* (3.128) and an identifiable *individual* (3.52) is removed where such an association may have existed

[SOURCE: ISO/IEC 15944-8:2012, 3.3.]

3.4
attribute
characteristic (3.14) of an *object* (3.73) or *entity* (3.43)

[SOURCE: ISO/IEC 15944-5:2008, 3.4]

3.5
authentication
provision of assurance of the claimed identity of an *entity* (3.43)

[SOURCE: ISO/IEC 10181-2:1996, 3.3]

3.6
back-up copy of data
copy that is any of the following: (a) additional resource or duplicate copy of *data* (3.28) on different a storage *medium* (3.68) stored off-line for emergency purposes; (b) disk, tape or other machine-readable copy of a data or program file; (c) data or program file recorded and stored off-line for emergency or archival purposes; and, (d) record that preserves the evidence and information it contains if the original is not available

3.7
business
series of *processes* (3.100), each having a clearly understood purpose, involving more than one *Person* (3.89), realized through the exchange of *recorded information* (3.110) and directed towards some mutually agreed upon goal, extending over a period of time

[SOURCE: ISO/IEC 14662:2010, 3.2]

3.8
business object
unambiguously (3.141) identified, specified, referenceable, registered and re-useable *Open-edi scenario* (3.81) or *scenario component* (3.124) of a *business transaction* (3.10)

Note 1 to entry: As an object, a business object exists only in the context of a business transaction.

[SOURCE: ISO/IEC 15944-2:2015, 3.6]

3.9
business operational view
BOV
perspective of *business transactions* (3.10) limited to those aspects regarding the making of *business* (3.7) decisions and *commitments* (3.20) among *Persons* (3.89), which are needed for the description of a business transaction

[SOURCE: ISO/IEC 14662:2010, 3.3]

3.10
business transaction
predefined set of activities and/or *processes* (3.100) of *Persons* (3.89) which is initiated by a *Person* to accomplish an explicitly shared *business* (3.7) goal and terminated upon recognition of one of the agreed conclusions by all the involved *Persons* although some of the recognition may be implicit

[SOURCE: ISO/IEC 14662:2010, 3.4]

3.11
business transaction audit trail
chronological record of *IT system* (3.59) activities that is sufficient to enable the reconstruction, reviewing and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event pertaining to *sets of recorded information (SRIs)* (3.128) in a *business transaction* (3.10) through all its *processes* (3.100), i.e., from planning to the end of post-actualization

Note 1 to entry: Note to entry: The ability to support a business transaction audit trail is required in order to be able to support privacy protection transactional integrity (PPTI) requirements.

3.12
business transaction identifier
BTI
identifier assigned by a *seller* (3.125) or a *regulator* (3.116) to an instantiated *business transaction* (3.10) among the *Persons* (3.89) involved

Note 1 to entry: The identifier assigned by the seller or regulator shall have the properties and behaviours of an identifier (in a business transaction).

Note 2 to entry: As an identifier (in a business transaction), a BTI 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 business transaction agreed to.

Note 3 to entry: A business 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 to entry: As and where required by the applicable jurisdictional domain(s), the recorded information associated with the business transaction identifier (BTI) may well require the seller to include other identifiers, (e.g., from a value-added good or service tax, etc., perspective) as assigned by the applicable jurisdictional domain(s).

[SOURCE: ISO/IEC 15944-5:2008, 3.12]

3.13
buyer
Person (3.89) 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

[SOURCE: ISO/IEC 15944-1:—, 3.8]

3.14
characteristic
abstraction of a *property* (3.102) of an *object* (3.73) or of a set of *objects*

Note 1 to entry: Characteristics are used for describing concepts.

[SOURCE: ISO 1087-1:2000, 3.2.4]

3.15
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/IEC 10646.

[SOURCE: ISO/IEC 2382:2015, 2121547]

3.16
code
<coded domain> identifier, i.e., an *ID code* (3.49), assigned to an *entity* (3.43) as member of a *coded domain* (3.17) according to the pre-established set of *rules* (3.120) governing that coded domain

[SOURCE: ISO/IEC 15944-5:2008, 3.19]

3.17
coded domain
domain for which (1) the boundaries are defined and explicitly stated as a *rulebase* (3.121) of a *coded domain source authority (cdSA)* (3.18); and, (2) each *entity* (3.43) 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 (RS)* (3.114) of that *source authority (SA)* (3.129)

Note 1 to entry: 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 (cdRS) of the source authority.

Note 2 to entry: Source authorities which are jurisdictional domains are the primary source of coded domains.

Note 3 to entry: 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 to entry: 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 to entry: In a coded domain the rules for assignment and structuring of the ID codes are required to be specified.

Note 6 to entry: 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 are required to be specified as the pivot ID code.

Note 7 to entry: 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 to entry: 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.

EXAMPLE 1 (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 to entry: In object methodology, entities which are members of a coded domain are referred to as instances of a class.

EXAMPLE 2 In UML modelling notation, an ID code is viewed as an instance of an object class.

[SOURCE: ISO/IEC 15944-2:2015, 3.13]

3.18
coded domain source authority
cdSA
Person (3.89), usually an *organization* (3.86), as a *source authority* (3.129) which sets the *rules* (3.120) governing a *coded domain* (3.17)

Note 1 to entry: 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 to entry: Specific sectors, (banking, transport, geomatics, agriculture, etc.), may have particular coded domain source authority(ies) whose coded domains are used in many other sectors.

Note 3 to entry: 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.

[SOURCE: ISO/IEC 15944-2:2015, 3.14]

3.19
collaboration space
business (3.7) activity space where an economic exchange of valued resources is viewed independently and not from the perspective of any *business* partner

Note 1 to entry: 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, etc. is not allowed because they view resource flows from a participant’s perspective.

[SOURCE: ISO/IEC 15944-4:2015, 3.12]

3.20
commitment
making or accepting of a right, obligation, liability or responsibility by a *Person* (3.89) that is capable of enforcement in the *jurisdictional domain* (3.62) in which the *commitment* (3.20) is made

[SOURCE: ISO/IEC 14662:2010, 3.5]

3.21
composite identifier
identifier (in business transaction) (3.51) functioning as a single unique identifier consisting of one or more other identifiers, and/or one or more other *data elements* (3.32), whose interworkings are rule-based

Note 1 to entry: Identifiers (in business transactions) are for the most part composite identifiers.

Note 2 to entry: The rules governing the structure and working of a composite identifier should be specified.

Note 3 to entry: Most widely used composite identifiers consist of the combinations of: (a) the ID of the overall identification/numbering schema (the ISO/IEC 6523 series, ISO/IEC 7812, the ISO/IEC 7501 series, UPC/EAN, ITU-T E.164, etc.), which is often assumed; (b) the ID of the issuing organization (often based on a block numeric numbering schema); and, (c) the ID of the entities forming part of members of the coded domain of each issuing organization.

[SOURCE: ISO/IEC 15944-2:2015, 3.16]

3.22
computational integrity
expression of a *standard* (3.137) 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 1 to entry: 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.

[SOURCE: ISO/IEC 15944-2:2015, 3.18]

3.23
constraint
rule (3.120), explicitly stated, that prescribes, limits, governs or specifies any aspect of a *business transaction* (3.10)

Note 1 to entry: 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 to entry: For constraints to be registered for implementation in Open-edi, they are required to have unique and unambiguous identifiers.

Note 3 to entry: 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.

[SOURCE: ISO/IEC 15944-1:—, 3.11]

3.24
consumer
buyer (3.13) who is an *individual* (3.52) to whom *consumer protection* (3.26) requirements are applied as a set of *external constraints* (3.45) on a *business transaction* (3.10)

Note 1 to entry: Consumer protection is a set of explicitly defined rights and obligations applicable as external constraints on a business transaction.

Note 2 to entry: 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 jurisdictional domain, such external constraints should be specified as part of scenario components as applicable.

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

[SOURCE: ISO/IEC 15944-1:—, 3.12]

3.25
consumer information profile
CIP
any one or more, *personal information profiles (PIPs)* (3.92) and any related *personal information* (3.90) on or about an identifiable *individual* (3.52) to which *consumer protection* (3.26) requirements apply, i.e., in addition to applicable *privacy protection* (3.97) requirements

3.26
consumer protection
set of *external constraints* (3.45) of a *jurisdictional domain* (3.62) as rights of a *consumer* (3.24) and thus as obligations (and possible liabilities) of a *vendor* (3.143) in a *business transaction* (3.10) which apply to the good, service and/or right forming the *object* (3.73) of the *business transaction* including associated information management and interchange requirements including applicable *set(s) of recorded information (SRIs)* (3.128)

Note 1 to entry: 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 to entry: 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 birthday).

Note 3 to entry: 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.

[SOURCE: ISO/IEC 15944-5:2008, 3.33]

3.27
controlled vocabulary
CV
vocabulary (3.144) whose entries, i.e., *definition* (3.37)/*term* (3.138) pairs, are controlled by a *source authority* (3.129) based on a *rulebase* (3.121) and *process* (3.100) for addition/deletion of entries

Note 1 to entry: In a controlled vocabulary (CV), there is a one-to-one relationship of definition and term.

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

Note 2 to entry: In a multilingual CV, the definition/term pairs in the languages used are deemed to be equivalent, i.e., with respect to their semantics.

Note 3 to entry: The rulebase governing a CV may include a predefined concept system.

[SOURCE: ISO/IEC 15944-5:2008, 3.34]

3.28
data
reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing

Note 1 to entry: Data can be processed by humans or by automatic means.

[SOURCE: ISO/IEC 2382:2015, 2122101]

3.29
data
<business transaction> representations of *recorded information* (3.110) that are being prepared or have been prepared in a form suitable for use in a computer system

[SOURCE: ISO/IEC 15944-1:—, 3.14]

3.30
data back-up
process (3.100) of duplicating and archiving *data* (3.28), often on a different storage *medium* (3.68), so that it may be restored to its original state after a data loss event

Note 1 to entry: The primary purpose of back-up is to recover data be it by data deletion or corruption.

Note 2 to entry: A secondary purpose of back-up is to be able to recover data from an earlier time according to a predefined retention policy.

3.31
data conversion
process (3.100) of changing *data* (3.28), i.e., as *set(s) of recorded information (SRI(s))* (3.128), from one format or representation to another while maintaining the *characteristics* (3.14) of the *SRIs* including the authenticity, integrity, reliability and usability of the *sets of recorded information (SRI(s))* as well as relevant *information life cycle management (ILCM)* (3.58) requirements, and especially those of an *external constraints* (3.45) nature including *privacy protection* (3.97) requirements where the *data* involves *personal information* (3.90)

Note 1 to entry: A characteristics of data conversion is a change in the format used for managing and/or representing the contents of the SRI.

EXAMPLE Data conversion resulting from a change in text processing software (e.g. Microsoft Word to HTML), from one database software to another, from a non-data based software to a database based software approach or vice-versa, etc.

Note 2 to entry: A data conversion does not change the content value of the SRI(s).

[SOURCE: Adapted from CAN/CGSB-72.34-2005, 3.16 and ISO 13008:2012, 3.5]

3.32
data element
unit of *data* (3.28) for which the *definition* (3.37), *identification* (3.50), representation and permissible values are specified by means of a set of *attributes* (3.4)

[SOURCE: ISO/IEC 15944-1:—, 3.15]

3.33
data migration
process (3.100) of moving *data* (3.28), i.e., as *sets of recorded information (SRIs)* (3.128) including their existing *characteristics* (3.14) from one *IT System* (3.59), (e.g., hardware or software configuration) to another, as required by changes in an *IT System* configuration or as requested by the user, while assuring that the *SRI(s)* will remain addressable and that data authenticity, integrity, reliability and usability of the *SRI(s)* will be maintained in the new environment

Note 1 to entry: Data migration does not change the content of the SRIs.

[SOURCE: Adapted from ISO 13008:2012, 3.12]

3.34
data synchronization
<business transaction> *process* (3.100) of continuous harmonization of a *set(s) of recorded information (SRI(s))* (3.128) among all the parties to a *business transaction* (3.10) to ensure that the current state of the content value(s) of such a *set(s) of recorded information (SRI(s))* is the same in the *IT systems* (3.59) of all the participating parties

[SOURCE: ISO/IEC 15944-8:2012, 3.35. Adapted from GS1 Global Traceability Standard (GDSN) Glossary.]

3.35
decision-making application
DMA
model (3.69) of that part of an *Open-edi system* (3.84) that makes decisions corresponding to the *role(s)* (3.119) that the *Open-edi Party* (3.78) plays as well as the originating, receiving and managing *data* (3.28) values contained in the instantiated *information bundles* (3.56) which is not required to be visible to the other *Open-edi Parties (OeP)*

[SOURCE: ISO/IEC 14662:2010, 3.7]

3.36
de facto language
natural language (3.72) used in a *jurisdictional domain* (3.62) 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 to entry: A de facto language of a jurisdictional domain is often established through long term use and custom.

Note 2 to entry: Unless explicitly stated otherwise and for the purposes of modelling a business 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.

[SOURCE: ISO/IEC 15944-5:2008, 3.42]

3.37
definition
representation of a concept by a descriptive statement which serves to differentiate it from related concepts

[SOURCE: ISO 1087-1:2000, 3.3.1]

3.38
designation
representation of a concept by a sign which denotes it

Note 1 to entry: In terminology work three types of designations are distinguished: symbols, appellations and terms.

[SOURCE: ISO/IEC 15944-2:2015, 3.79.]

3.39
eBusiness
business transaction (3.10), involving the making of *commitments* (3.20), in a defined *collaboration space* (3.19), among *Persons* (3.89) using their *IT systems* (3.59), according to *Open-edi standards* (3.82)

Note 1 to entry: eBusiness can be conducted on both a for-profit and not-for-profit basis.

Note 2 to entry: 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 to entry: eBusiness includes various application areas such as e-commerce, e-administration, e-logistics, e-government, e-medicine, e-learning, etc.

Note 4 to entry: The equivalent French language term for “eBusiness” is always presented in its plural form.

[SOURCE: ISO/IEC 15944-7:2009, 3.06]

3.40
electronic address
address (3.1) used in a recognized electronic addressing scheme (telephone, telex, IP, etc.), to which *recorded information* (3.110) item(s) and/or *business object(s)* (3.8) can be sent to or received from a contact

[SOURCE: ISO/IEC 15944-2:2015, 3.32]

3.41
electronic data interchange
EDI
automated exchange of any predefined and structured *data* (3.28) for *business* (3.7) purposes among information systems of two or more *Persons* (3.89)

Note 1 to entry: This definition includes all categories of electronic business transactions.

[SOURCE: ISO/IEC 14662:2010, 3.8]

3.42
electronic signature
signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with a particular digital/electronic *set of recorded information (SRI)* (3.128)

Note 1 to entry: A Person signature may be in the form of an electronic signature or not.

[SOURCE: Adapted from PIPEDA, Part 2, section 31(1); CAN/CGSB-72.34-2005, 3.28.]

3.43
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 1 to entry: An entity exists whether data about it are available or not.

[SOURCE: ISO/IEC 2382:2015, 2121433]

3.44
expungement
process (3.100) of ensuring complete elimination, wiping out, destroying, or obliteration of any *recorded information* (3.110) [or *sets of recorded information (SRIs)*] (3.128), often including the *medium* (3.68) on which it is recorded, so that there can be no reconstruction of any its contents in whole or in part

3.45
external constraint
constraint (3.23) which takes precedence over *internal constraints* (3.60) in a *business transaction* (3.10), i.e., is external to those agreed upon by the parties to a business transaction

Note 1 to entry: Normally external constraints are created by law, regulation, orders, treaties, conventions or similar instruments.

Note 2 to entry: 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, (INCOTERMS, exchanges, etc.).

Note 3 to entry: External constraints can apply to the nature of the good, service and/or right provided in a business transaction.

Note 4 to entry: External constraints can demand that a party to a business 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 to entry: Where the information bundles (IBs), including their semantic components (SCs) of a business transaction are also to form the whole of a business transaction, (e.g., for legal or audit purposes), all constraints are required to be recorded.

EXAMPLE 4 There may be a legal or audit requirement to maintain the complete set of recorded information pertaining to a business transaction, i.e., as the Information Bundles exchanged, as a record.

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

[SOURCE: ISO/IEC 15944-1:—, 3.23]

3.46
formal description technique
FDT
specification method based on a description *language* (3.63) using rigorous and *unambiguous* (3.141) *rules* (3.120) both with respect to developing expressions in the *language* (formal syntax) and interpreting the meaning of these expressions (formal semantics)

[SOURCE: ISO/IEC 14662:2010, 3.9]

3.47
functional service view
FSV
perspective of *business transactions* (3.10) limited to those information technology interoperability aspects of *IT Systems* (3.59) needed to support the execution of *Open-edi transactions* (3.85)

[SOURCE: ISO/IEC 14662:2010, 3.10]

3.48
human interface equivalent
HIE
representation of the *unambiguous* (3.141) and IT-enabled semantics of an IT interface equivalent (in a *business transaction* (3.10)), often the *ID code* (3.49) of a *coded domain* (3.17) (or a *composite identifier* (3.21)), in a formalized manner suitable for communication to and understanding by humans

Note 1 to entry: Human interface equivalents can be linguistic or non-linguistic in nature but their semantics remain the same although their representations may vary.

Note 2 to entry: In most cases there will be multiple human interface equivalent representations as required to meet localization requirements, i.e., those of a linguistic, jurisdictional, and/or sectoral nature.

Note 3 to entry: Human interface equivalents include representations in various forms or formats [in addition to written text those of an audio, symbol (and icon) nature, glyphs, image, etc.].

[SOURCE: ISO/IEC 15944-2:2015, 3.35]

3.49
ID code
identifier assigned by the *coded domain source Authority (cdSA)* (3.18) to a member of a *coded domain* (3.17) ID

Note 1 to entry: ID codes should be unique within the registration schema of that coded domain.

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

Note 3 to entry: 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 should be specified as the pivot ID code.

Note 4 to entry: 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 should be predefined and explicitly stated.

EXAMPLE (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 to entry: In UML modelling notation, an ID codes is viewed as an instance of an object class.

[SOURCE: ISO/IEC 15944-2:2015, 3.37]

3.50
identification
rule-based *process* (3.100), explicitly stated, involving the use of one or more *attributes* (3.4), i.e., *data element(s)* (3.32), whose value (or combination of values) are used to identify uniquely the occurrence or existence of a specified *entity* (3.43)

[SOURCE: ISO/IEC 15944-1:—, 3.26]

3.51
identifier
<business transaction> *unambiguous* (3.141), unique and a linguistically neutral value, resulting from the application of a rule-based *identification* (3.50) *process* (3.100)

Note 1 to entry: Identifiers are required to be unique within the identification scheme of the issuing authority.

Note 2 to entry: An identifier is a linguistically independent sequence of characters capable of uniquely and permanently identifying that with which it is associated [see ISO 19135:2015 (4.1.5)].

[SOURCE: ISO/IEC 15944-1:—, 3.27]

3.52
individual
Person (3.89) who is a human being, i.e., a natural person, who acts as a distinct indivisible *entity* (3.43) or is considered as such

[SOURCE: ISO/IEC 15944-1:—, 3.28]

3.53
individual accessibility
set of *external constraints* (3.45) of a *jurisdictional domain* (3.62) as rights of an *individual* (3.52) with disabilities to be able to use *IT Systems* (3.59) at the human, i.e., user, interface and the concomitant obligation of a *seller* (3.125) to provide such adaptive technologies

Note 1 to entry: Although accessibility typically addresses users who have a disability, the concept is not limited to disability issues.

EXAMPLE Disabilities in the form of functional and cognitive limitations include: (a) people who are blind; (b) people with low vision; (c) people with colour blindness; (d) people who are hard of hearing or deaf, i.e., are hearing impaired; (e) people with physical disabilities; and, (f) people with language or cognitive disabilities.

[SOURCE: ISO/IEC 15944-5:2008, 3.60]

3.54
individual anonymity
state of not knowing the identity or not having any recording of *personal information* (3.90) on or about an *individual* (3.52) as a *buyer* (3.13) by the *seller* (3.125) or *regulator* (3.116), (or any other party) to a *business transaction* (3.10)

[SOURCE: ISO/IEC 15944-8:2012, 3.57]

3.55
individual identity
ii
Person identity (Pi) (3.93) of an *individual* (3.52) consisting of the combination of the *persona* (3.95) information and *identifier* used by an individual in a *business transaction* (3.10), i.e., in the making of any kind of *commitment* (3.20)

[SOURCE: ISO/IEC 15944-8:2017, 3.59]

3.56
information bundle
IB
formal description of the semantics of the *recorded information* (3.110) to be exchanged by *Open-edi parties* (3.78) playing *roles* (3.119) in an *Open-edi scenario* (3.81)

[SOURCE: ISO/IEC 14662:2010, 3.11]

3.57
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* (3.110), 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*

[SOURCE: ISO/IEC 15944-8:2012, 3.62]

3.58
information life cycle management
ILCM
series of actions and *rules* (3.120) governing the management and its *electronic data interchange (EDI)* (3.41) of *set(s) of recorded information (SRIs)* (3.128) *under the control of* (3.142) a *Person* (3.89) from its creation to final disposition, including *expungement* (3.44), in compliance with applicable *information law* (3.57) requirements

Note 1 to entry: The inclusion of information law brings into this definition all the resulting various information management requirements and related activities.

3.59
information technology system
IT System
set of one or more computers, associated software, peripherals, terminals, human operations, physical *processes* (3.100), information transfer means, that form an autonomous whole, capable of performing information processing and/or information transfer

[SOURCE: ISO/IEC 14662:2010, 3.13]

3.60
internal constraint
constraint (3.23) which forms part of the *commitment(s)* (3.20) mutually agreed to among the parties to a *business transaction* (3.10)

Note 1 to entry: Internal constraints are self-imposed. They provide a simplified view for modelling and re-use of scenario components of a business transaction for which there are no external constraints or restrictions to the nature of the conduct of a business transaction other than those mutually agreed to by the buyer and seller.

[SOURCE: ISO/IEC 15944-1:—, 3.33]

3.61
IT-enablement
transformation of a current *standard* (3.137) used in *business transactions* (3.10), (e.g., *coded domains* (3.17)), from a manual to computational perspective so as to be able to support *commitment* (3.20) exchange and *computational integrity* (3.22)

[SOURCE: ISO/IEC 15944-5:2008, 3.65]

3.62
jurisdictional domain
jurisdiction, recognized in law as a distinct legal and/or regulatory framework, which is a source of *external constraints* (3.45) on *Persons* (3.89), their behaviour and the making of *commitments* (3.20) among *Persons* including any aspect of a *business transaction* (3.10)

Note 1 to entry: The pivotal 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 to entry: Jurisdictional domains can combine to form new jurisdictional domains, (e.g., through bilateral, multilateral and/or international treaties).

EXAMPLE European Union (EU), NAFTA, WTO, WCO, ICAO, WHO, Red Cross, ISO, IEC, ITU-T.

Note 3 to entry: Several levels and categories of jurisdictional domains may exist within a jurisdictional domain.

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

Note 5 to entry: 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 business transactions.

[SOURCE: ISO/IEC 15944-5:2008, 3.67]

3.63
language
system of signs for communication, usually consisting of a *vocabulary* (3.144) and *rules* (3.120)

Note 1 to entry: In this document, language refers to natural languages or special languages, but not "programming languages" or "artificial languages".

[SOURCE: ISO 5127:2017, 11.2.01]

3.64
legally recognized name
LRN
persona associated with a *role* (3.119) of a *Person* (3.89) recognized as having legal status and so recognized in a *jurisdictional domain* (3.62) as accepted or assigned in compliance with the *rules* (3.120) applicable of that *jurisdictional domain*, i.e., as governing the *coded domain* (3.17) of which the *legally recognized name (LRN)* (3.64) is a member

Note 1 to entry: 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 to entry: The process of the establishment of a LRN is usually accompanied by the assignment of a unique identifier.

Note 3 to entry: 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 to entry: A Person may have more than one LRN (and associated LRN identifier).

[SOURCE: ISO/IEC 15944-5:2008, 3.72]

3.65
list
ordered set of *data elements* (3.32)

[SOURCE: ISO/IEC 15944-5:2008, 3.73]

3.66
localization
pertaining to or concerned with anything that is not global and is bound through specified sets of *constraints* (3.23) of: (a) a linguistic nature including *natural language* (3.72) and *special languages* (3.130) 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* (3.24) behaviour requirements; and/or, (f) safety or health requirements

Note 1 to entry: Within and among "locales", interoperability and harmonization objectives also apply.

[SOURCE: ISO/IEC 15944-5:2008, 3.75]

3.67
location
place, either physical or electronic, that can be defined as an *address* (3.1)

[SOURCE: ISO/IEC 15944-2:2015, 3.50]

3.68
medium
physical material which serves as a functional unit, in or on which information or *data* (3.28) 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 to entry: 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 to entry: The inclusion of the "non-volatile in nature" attribute is to cover latency and records retention requirements.

Note 3 to entry: This definition of medium is independent of: (a) the form or format of recorded information; (b) the physical dimension and/or size; and, (c) any container or housing that is physically separate from material being housed and without which the medium can remain a functional unit.

Note 4 to entry: This definition of medium also captures and integrates the following key properties: (a) the property of medium as a material in or on which information or data can be recorded and retrieved; (b) the property of storage; (c) the property of physical carrier; (d) the property of physical manifestation, i.e., material; (e) the property of a functional unit; and, (f) the property of (some degree of) stability of the material in or on which the information or data is recorded.

[SOURCE: ISO/IEC 15944-1:—, 3.34]

3.69
model
abstraction of some aspect of reality

[SOURCE: ISO 19115:2014, 4.9]

3.70
multilingualism
ability to support not only *character sets* (3.15) specific to a (*natural*) *language* (or family of *languages* (3.63)) and associated *rules* (3.120) but also *localization* (3.66) requirements, i.e., use of a language from *jurisdictional domain* (3.62), sectoral and/or *consumer* (3.24) marketplace perspectives

[SOURCE: ISO/IEC 15944-5:2008, 3.82]

3.71
name
designation (3.38) of an *object* (3.73) by a linguistic expression

[SOURCE: ISO/IEC 15944-1:—, 3.35.]

3.72
natural language
language (3.63) which is or was in active use in a community of people, and the *rules* (3.120) of which are mainly deduced from the usage

[SOURCE: ISO 5127:2017, 3.1.5.2]

3.73
object
anything perceivable or conceivable

Note 1 to entry: 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).

[SOURCE: ISO 1087-1:2000, 3.1.1]

3.74
object class
set of ideas, abstractions, or things in the real world that can be identified with explicit boundaries and meaning and whose *properties* (3.102) and behaviour follow the same *rules* (3.120)

[SOURCE: ISO/IEC 11179-1:2015, 3.3.18]

3.75
official language
external constraint (3.45) in the form of a *natural language* (3.72) specified by a *jurisdictional domain* (3.62) for official use by *Persons* (3.89) forming part of and/or subject to that jurisdictional domain for use in communication(s) either: (a) within that *jurisdictional domain*; and/or, (b) among such *Persons*, where such communications are *recorded information* (3.110) involving *commitment(s)* (3.20)

Note 1 to entry: 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 to entry: A jurisdictional domain decides whether or not it has an official language. If not, it will have a de facto language.

Note 3 to entry: 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 to entry: 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 to entry: 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 is required to be specified.

Note 6 to entry: 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 Norway has two official writing systems, both Latin-1 based, namely, Bokmål (Dano-Norwegian) and Nynorsk (New Norwegian).

Note 7 to entry: A jurisdictional domain may have more than one official language but these may or may not have equal status.

EXAMPLE 3 Canada has two official languages, Switzerland has three, while the Union of South Africa has eleven official languages.

Note 8 to entry: The BOV requirement of the use of a specified language will place that requirement on any FSV supporting service.

EXAMPLE 4 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.

[SOURCE: ISO/IEC 15944-5:2008, 3.87]

3.76
Open-edi
electronic data interchange (3.41) *(EDI)* among multiple autonomous *Persons* (3.89) to accomplish an explicit shared *business* (3.7) goal according to *Open-edi standards* (3.82)

[SOURCE: ISO/IEC 14662:2010, 3.14]

3.77
Open-edi disposition
process (3.100) governing the implementation of formally approved records retention, destruction (or *expungement* (3.44)) or transfer of *recorded information* (3.110) *under the control of* (3.142) a *Person* (3.89) which are documented in a records scheduling and disposition authority(ies) or similar instrument of the *organization* (3.86)

Note 1 to entry: Within an organization, Open-edi disposition shall be in accordance and compliant with the applicable Open-edi records retention (OeRR) and disposal schedule (RRDS) of the organization.

[SOURCE: ISO/IEC 15944-5:2008, 3.90]

3.78
Open-edi party
OeP
Person (3.89) that participates in *Open-edi* (3.76)

Note 1 to entry: Often referred to generically in this and other eBusiness standards, (e.g., parts of the ISO/IEC 15944 series) as party or parties for any entity modelled as a Person as playing a role in Open-edi scenarios.

[SOURCE: ISO/IEC 14662:2010, 3.17]

3.79
Open-edi record retention
OeRR
specification of a period of time that a *set of recorded information (SRI)* (3.128) is required to be kept by a *Person* (3.89) in order to meet operational, legal, regulatory, fiscal or other requirements as specified in the *external constraints* (3.45) (or *internal constraints* (3.60)) applicable to a *Person* who is a party to a *business transaction* (3.10)

[SOURCE: ISO/IEC 15944-5:2008, 3.92]

3.80
Open-edi registry item
OeRI
recorded information (3.110) within a *registry* (3.115) relating to a specific *Open-edi scenario* (3.81) or *scenario components* (3.124) of a *scenario* (3.122) including linkage information to a *scenario* content

[SOURCE: ISO/IEC 15944-2:2015, 3.70]

3.81
Open-edi scenario
OeS
formal specification of a class of *business transactions* (3.10) having the same *business* (3.7) goal

[SOURCE: ISO/IEC 14662:2010, 3.18]

3.82
Open-edi standard
standard (3.137) that complies with the *Open-edi* (3.76) reference model

[SOURCE: ISO/IEC 14662:2010, 3.19]

3.83
Open-edi support infrastructure
OeSI
model (3.69) of the set of functional capabilities for *Open-edi systems* (3.84) which, when taken together with the *decision-making applications* (3.35), allows *Open-edi* (3.76) parties to participate in *Open-edi transactions* (3.85)

[SOURCE: ISO/IEC 14662:2010, 3.20]

3.84
Open-edi system
information technology system (IT system) (3.59) which enables an *Open-edi party* (3.78) to participate in *Open-edi transactions* (3.85)

[SOURCE: ISO/IEC 14662:2010, 3.22]

3.85
Open-edi transaction
business transaction (3.10) that is in compliance with an *Open-edi scenario* (3.81)

[SOURCE: ISO/IEC 14662:2010, 3.23]

3.86
organization
unique framework of authority within which a person or persons act, or are designated to act, towards some purpose

Note 1 to entry: 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, services and/or rights including: (a) partnerships; (b) social or other non-profit organizations or similar bodies in which ownership or control is vested in a group of individuals; (c) sole proprietorships; and, (d) governmental bodies.

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

[SOURCE: ISO/IEC 15944-1:—, 3.44.]

3.87
organization part
any department, service or other *entity* (3.43) within an *organization* (3.86), which needs to be identified for information interchange

[SOURCE: ISO/IEC 6523-1:1998, 3.2]

3.88
organization Person
organization part (3.87) which has the *properties* (3.102) of a *Person* (3.89) and thus is able to make *commitments* (3.20) on behalf of that *organization* (3.86)

Note 1 to entry: An organization can have one or more organization Persons.

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

Note 3 to entry: An organization Person can be a natural person such as an employee or officer of the organization.

Note 4 to entry: An organization Person can be a legal person, i.e., another organization.

[SOURCE: ISO/IEC 15944-1:—, 3.46]

3.89
Person
entity (3.43), i.e., a natural or legal person, recognized by law as having legal rights and duties, able to make *commitment(s)* (3.20), assume and fulfil resulting obligation(s), and able of being held accountable for its action(s)

Note 1 to entry: Synonyms for "legal person" include "artificial person", "body corporate", etc., depending on the terminology used in competent jurisdictional domains.

Note 2 to entry: 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 to entry: Minimum and common external constraints applicable to a business transaction often require one to differentiate among three common sub-types of Person, namely individual, organization, and public administration.

[SOURCE: ISO/IEC 14662:2010, 3.24]

3.90
personal information
PI
any information on or about an identifiable *individual* (3.52) that is recorded in any form, including electronically or on paper

EXAMPLE Recorded information about an individual's religion, age, financial transactions, medical history, address, or blood type.

[SOURCE: ISO/IEC 15944-5:2008, 3.103]

3.91
personal information controller
PIC
organization Person (3.88) authorized and so formally designated by the *organization* (3.86) to ensure that *personal information* (3.90) remains (fully) *under the control of* (3.142) the *organization* and ensures its *privacy protection transactional integrity (PPTI)* (3.99) in compliance with applicable *privacy protection* (3.97) requirements including in any use by the *organization* of *agents* (3.2) and/or *third parties* (3.139) in support of a *business transaction(s)* (3.10)

Note 1 to entry: The primary role and responsibility pertain to and focus on ensuring that: (a) personal information remains under the control of the organization; and, (b) required ILCM aspects are implemented in a verifiable manner. A PIC also bridges the BOV-to-FSV with respect to all aspects of information handling (processing and EDI) of personal information of IT system(s) of an organization.

Note 2 to entry: A PIC has a defined set of responsibilities which can be "outsourced" should a seller decide to use an agent and/or third party based on a contractual agreement to ensure that the privacy protection requirements (rights) of the buyer as an individual are fully supported.

Note 3 to entry: An organization may authorize and designate its privacy protection officer (PPO) to also function in the role of its personal information controller (PIC).

Note 4 to entry: A privacy protection officer (PPO) is a role of an officer in an organization. It may well be that the same organization Person is assigned responsibility for more than one role within an organization including those pertaining to corporate information law compliance, responsibility for corporate internal constraints such as information/records management, security, etc.

3.92
personal information profile
PIP
any collection of *personal information (PI)* (3.90) or aggregation of *sets of personal information (SPIs)* (3.127) including associated identifiers, linkages and/or associations, on or about an identifiable *individual* (3.52) being collected, retained, managed, used, etc., by any other *Person* (3.89) and in particular an *organization* (3.86) *or public administration* (3.105) and as such to which *privacy protection* (3.97) requirements apply including those of a *ILCM* (3.58) nature

Note 1 to entry: A personal information profile (PIP) includes any personal information (PI) created by the seller (and parties acting on its behalf such as an agent) in the instantiated business transaction, (e.g., in the post-actualization phase assigning an applicable warranty for the good, service and/or right purchased to another individual where the original buyer (as an individual) "gifts" the good to another individual.

Note 2 to entry: A personal information profile (PIP) often includes personal information (PI) resulting from more than one instantiated business transaction.

3.93
Person identity
Pi
combination of *persona* (3.95) information and *identifier* (3.51) used by a *Person* (3.89) in a *business transaction* (3.10)

[SOURCE: ISO/IEC 15944-1:—, 3.49]

3.94
Person signature
signature, i.e., a *name* (3.71) representation, distinguishing mark or usual mark, which is created by and pertains to a *Person* (3.89)

[SOURCE: ISO/IEC 15944-1:—, 3.50]

3.95
persona
set of *data elements* (3.32) and their values by which a *Person* (3.89) wishes to be known and thus identified in a *business transaction* (3.10)

[SOURCE: ISO/IEC 15944-1:—, 3.51]

3.96
principle
fundamental, primary assumption and quality which constitutes a source of action determining particular objectives or results

Note 1 to entry: A principle is usually enforced by rules that affect its boundaries.

Note 2 to entry: A principle is usually supported through one or more rules.

Note 3 to entry: 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.

[SOURCE: ISO/IEC 15944-2:2015, 3.81]

3.97
privacy protection
set of *external constraints* (3.45) of a *jurisdictional domain* (3.62) pertaining to *recorded information* (3.110) on or about an identifiable *individual* (3.52), i.e., *personal information* (3.90), 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 to entry: Recorded information collected or created for a specific purpose on an identifiable individual, i.e., the explicitly shared goal of the business 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 to entry: Privacy protection requirements include the right of an individual to be able to view the recorded information about him/herself and to request corrections to the same in order to ensure that such recorded information is accurate and up-to-date.

Note 3 to entry: Where jurisdictional domains have legal requirements which override privacy protection requirements these are required to be specified, (e.g., national security, investigations by law enforcement agencies, etc.).

[SOURCE: ISO/IEC 15944-5:2008, 3.109]

3.98
privacy protection officer
PPO
organization Person (3.88) authorized by the *organization* (3.86) 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* (3.97) requirements for *information life cycle management* (3.58) not only within that *organization* but also with respect to any *electronic data interchange* (3.41) of *personal information* (3.90) on the *individual* (3.52) concerned with parties to the *business transaction* (3.10), including a *regulator* (3.116) where required, as well as any *agents* (3.2), *third parties* (3.139) involved in that *business transaction*

[SOURCE: ISO/IEC 15944-8:2012, 3.115]

3.99
privacy protection transactional integrity
PPTI
process (3.100) of ensuring that the *seller* (3.125) ensures that *data synchronization (in business transaction)* (3.34) requirements among the *IT systems* (3.59) of all parties to a *business transaction* (3.10) conform to, and are compliant with, applicable *privacy protection* (3.97) requirements (PPR) of (all) the *jurisdictional domain(s)* (3.62) applicable to that instantiated *business transaction* where and whenever such a business transaction involves a *buyer* (3.13) as an *individual* (3.52), i.e., whenever any part of the *recorded information* (3.110) of that *business transaction* involves *personal information (PI)* (3.90)

Note 1 to entry: The concept and requirement of transactional integrity which focuses on EDI among IT systems is based on the requirements for referential integrity within an IT system of an organization.

3.100
process
series of actions or events taking place in a defined manner leading to the accomplishment of an expected result

[SOURCE: ISO/IEC 15944-1:—, 3.53]

3.101
processing of personal information
any operation or set of operations which is performed upon *personal information* (3.90), 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, destruction, or expungement of such *personal information*

[SOURCE: ISO/IEC 15944-8:2012, 117]

3.102
property
peculiarity common to all members of an *object class* (3.74)

[SOURCE: ISO/IEC 15944-5:2008, 3.111]

3.103
pseudonym
use of a *persona* or other identifier by an *individual* (3.52) which is different from that used by the *individual* (3.52) with the intention that it be not linkable to that *individual* (3.52)

[SOURCE: ISO/IEC 15944-8:2012, 3.119]

3.104
pseudonymization
particular type of *anonymization* (3.3) that removes the association with an *individual* (3.52) and adds an association between a particular set of *characteristics* (3.14) relating to the *individual* and one more *pseudonym* (3.103)

[SOURCE: ISO/IEC 15944-8:2012, 3.120.]

3.105
public administration
entity (3.43), i.e., a *Person* (3.89), which is an *organization* (3.86) and has the added *attribute* (3.4) of being authorized to act on behalf of a *regulator* (3.116)

[SOURCE: ISO/IEC 15944-1:—, 3.54]

3.106
public policy
category of *external constraints* (3.45) of a *jurisdictional domain* (3.62) specified in the form of a right of an *individual* (3.52) or a requirement of an *organization* (3.86) and/or *public administration* (3.105) with respect to an *individual* pertaining to any exchange of *commitments* (3.20) among the parties concerned involving a good, service and/or right including information management and interchange requirements

Note 1 to entry: Public policy requirements may apply to any one, all or combinations of the fundamental activities comprising a business transaction, i.e., planning, identification, negotiation, actualization and post-actualization (see further ISO/IEC 15944-1:—, 6.3).

Note 2 to entry: 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 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 to entry: Jurisdictional domains may have consumer protection or privacy protection requirements which apply specifically to individuals who are considered to be children, minors, etc., i.e., those who have not reached their 18th or 21st birthday according to the rules of the applicable jurisdictional domain.

[SOURCE: ISO/IEC 15944-5:2008, 3.113]

3.107
publicly available personal information
PAPI
personal information (3.90) about an *individual* (3.52) that the *individual* knowingly makes or permits to be made available to the public, or is legally obtained and accessed from: (1) government records that are available to the public; or, (2) information required by law to be made available to the public

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

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

[SOURCE: ISO/IEC 15944-8:2012, 3.123]

3.108
recognized individual identity
rii
individual identity (ii) (3.55) established to the extent necessary for the specific purpose of a *business transaction* (3.10)

[SOURCE: ISO/IEC 15944-8:2012, 3.124]

3.109
recognized Person identity
rPi
Person identity (Pi) (3.93), established to the extent necessary for a specific purpose in a *business transaction* (3.10)

[SOURCE: ISO/IEC 15944-1:—, 3.56]

3.110
recorded information
information that is recorded on or in a *medium* (3.68) irrespective of form, recording *medium* or technology used, and in a manner allowing for storage and retrieval

Note 1 to entry: 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 to entry: Through the use of the term "information," all attributes of this term are inherited in this definition.

Note 3 to entry: This definition covers: (a) any form of recorded information, means of recording, and any medium on which information can be recorded; and, (b) all types of recorded information including all data types, instructions or software, databases, etc.

[SOURCE: ISO/IEC 15944-1:—, 3.56]

3.111
register
set of files containing identifiers assigned to items with descriptions of the associated items

[SOURCE: ISO 19135-1:2015, 4.1.9]

3.112
registration
rule-based *process* (3.100), explicitly stated, involving the use of one or more *data elements* (3.32), whose value (or combination of values) is used to identify uniquely the results of assigning an *Open-edi registry item (OeRI)* (3.80)

[SOURCE: ISO/IEC 15944-2:2015, 3.95]

3.113
registration authority
RA
Person (3.89) responsible for the maintenance of one or more *registration schemas (RS)* (3.114) including the assignment of a unique identifier for each recognized *entity* (3.43) in a *registration schema (RS)*

[SOURCE: ISO/IEC 15944-1:—, 3.57]

3.114
registration schema
RS
formal *definition* (3.37) of a set of *rules* (3.120) governing the *data* (3.28) fields for the description of an *entity* (3.43) and the allowable contents of those fields, including the rules for the assignment of *identifiers* (3.51)

[SOURCE: ISO/IEC 15944-1:—, 3.58]

3.115
registry
information system on which a *register* (3.111) is maintained

[SOURCE: ISO/IEC 15944-2:2015, 3.99]

3.116
regulator
Person (3.89) who has authority to prescribe *external constraints* (3.45) which serve as *principles* (3.96), policies or *rules* (3.120) governing or prescribing the behaviour of *Persons* involved in a *business transaction* (3.10) as well as the provisioning of goods, services, and/or rights interchanged

[SOURCE: ISO/IEC 15944-1:—, 3.59]

3.117
regulatory business transaction
RBT
class of *business transactions* (3.10) for which the explicitly shared goal has been established and specified by a *jurisdictional domain* (3.62), as a *Person* (3.89) in the *role* (3.119) of a *regulator* (3.116)

Note 1 to entry: A regulatory business transaction (RBT) can itself be modelled as a stand-alone business transaction and associated scenario(s).

EXAMPLE The filing of a tax return, the making of a customs declaration, the request for and issuance of a licence, the provision of a specified service of a public administration, a mandatory filing of any kind with a regulator, etc.

Note 2 to entry: A regulatory business transaction (modelled as a scenario) can form part of another business transaction.

Note 3 to entry: A RBT may apply to a seller only, a buyer only or both, as well as any combination of parties to a business transaction.

Note 4 to entry: A RBT may require or prohibit the use of an agent or third party.

Note 5 to entry: A regulatory business transaction (RBT) may be specific to the nature of the good, services and/or right forming part of a business transaction.

[SOURCE: ISO/IEC 15944-5:2008, 3.124]

3.118
retention period
length of time for which *data* (3.28) on a *data medium* (3.68) is to be preserved

[SOURCE: ISO/IEC 15944-5:2008, 3.136]

3.119
role
specification which models an external intended behaviour (as allowed within a scenario) of an *Open-edi party* (3.78)

[SOURCE: ISO/IEC 14662:2010, 3.25]

3.120
rule
statement governing conduct, procedure, conditions and relations

Note 1 to entry: Rules specify conditions that should be complied with. These may include relations among objects and their attributes.

Note 2 to entry: Rules are of a mandatory or conditional nature.

Note 3 to entry: 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) business 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 to entry: Rules should be clear and explicit enough to be understood by all parties to a business transaction. Rules also should 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)".

[SOURCE: ISO/IEC 15944-2:2015, 3.101]

3.121
rulebase
pre-established set of *rules* (3.120) which interwork and which together form an autonomous whole

Note 1 to entry: One considers a rulebase to be to rules as database is to data.

[SOURCE: ISO/IEC 15944-2:2015, 3.102]

3.122
scenario
formal specification of a class of *business* (3.7) activities having the same business goal

[SOURCE: ISO 9735-1:2002, 4.89]

3.123
scenario attribute
formal specification of information, relevant to an *Open-edi scenario* (3.81) as a whole, which is neither specific to *roles* (3.119) nor to *Information Bundles* (3.56)

[SOURCE: ISO/IEC 14662:2010, 3.26]

3.124
scenario component
one of the three fundamental elements of a scenario, namely *role* (3.119), *information bundle* (3.56), and *semantic component* (3.126)

[SOURCE: ISO/IEC 15944-2:2015, 3.104]

3.125
seller
Person (3.89) 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

[SOURCE: ISO/IEC 15944-1:—, 3.62]

3.126
semantic component
SC
unit of *recorded information* (3.110) *unambiguously* (3.141) defined in the context of the *business* (3.7) goal of the *business transaction* (3.10)

Note 1 to entry: A SC may be atomic or composed of other SCs.

[SOURCE: ISO/IEC 14662:2010, 3.27]

3.127
set of personal information
SPI
set of *recorded information (SRI)* (3.128) which is of the nature of, or contains, *personal information* (3.90)

3.128
set of recorded information
SRI
recorded information (3.110) of a *Person* (3.89), which is *under the control of* (3.142) the same and which is treated as a unit in its information life cycle

Note 1 to entry: 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 to entry: 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 to entry: 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.

[SOURCE: ISO/IEC 15944-5:2008, 3.137]

3.129
source authority
SA
Person (3.89) recognized by other *Persons* as the authoritative source for a set of *constraints* (3.23)

Note 1 to entry: A Person as a source authority for internal constraints may be an individual, organization, or public administration.

Note 2 to entry: 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 to entry: A Person as an individual shall not be a source authority for external constraints.

Note 4 to entry: Source authorities are often the issuing authority for identifiers (or composite identifiers) for use in business transactions.

Note 5 to entry: A source authority can undertake the role of registration authority or have this role undertaken on its behalf by another Person.

Note 6 to entry: Where the sets of constraints of a source authority control a coded domain, the SA has the role of a coded domain source authority.

[SOURCE: ISO/IEC 15944-2:2015, 3.109]

3.130
special language
language (3.63) for special purposes (LSP), language used in a subject field and characterized by the use of specific linguistic means of expression

Note 1 to entry: The specific linguistic means of expression always include subject-specific terminology and phraseology and also may cover stylistic or syntactic features.

[SOURCE: ISO/IEC 15944-5:2008, 3.139]

3.131
SPI expungement
process (3.100) of ensuring *expungement* (3.44) of a *set of personal information (SPI)* (3.127) in accordance with *privacy protection* (3.97) laws and regulations of the applicable *jurisdictional domain* (3.62)

Note 1 to entry: In a business transaction the seller shall ensure that all parties to the business transaction including agents, and/or third parties with whom such a set(s) of personal information was exchanged are also expunged, i.e., as part of ensuring transactional integrity.

3.132
SRI custody
association between a *Person* (3.89) having physical or virtual possession of a *set(s) of recorded information (SRIs)* (3.128) in the *role* (3.119) of an *agent* (3.2) or a *third party* (3.139) on behalf of the *Person* who is responsible for *under the control of* (3.142) associated legal/regulatory requirements pertaining to the *SRI(s)*, in particular *privacy protection* (3.97) requirements

Note 1 to entry: On the whole, the default is that of the SRI pertaining to any business transaction as being the Person in the role of seller for the instantiation of that business transaction.

3.133
SRI destruction
process (3.100) of eliminating or deleting a *set of recorded information* (3.128), beyond any possible reconstruction

3.134
SRI integrity
reliability and trustworthiness of a *set(s) of recorded information (SRI(s))* (3.128), as well as of any as copies, duplicates or comparable representations of the *SRI(s)*; and reliability and trustworthiness of the *IT system(s)* (3.59) in which the *SRI(s)* were recorded or stored to produce reliable and trustworthy copies and duplicates of *set(s) of recorded information (SRI(s))*

Note 1 to entry: SRI integrity is important in the electronic records provisions of the evidence acts in the phrases "the integrity of the electronic records system" and "the integrity of the electronic record." However, the term integrity is not defined in rules governing forensic data in 'evidence acts'. In the absence of a statutory or judicially created definition, the principles of this document shall serve as an operational definition of the word "integrity" when used in the context of 'evidence acts'.

Note 2 to entry: Certain evidence acts provide that the integrity of the electronic record may be proved by evidence of reliable and adequately implemented encryption.

Note 3 to entry: Organizations which implement the requirements of the rules (and associated guidelines) pertaining to records retention requirements and state changes to the content values of an SRI, as defined in Tables 1–7 are deemed to meet basic SRI integrity requirements.

3.135
SRI life cycle
stages in the life cycle of a *set of recorded information (SRI)* (3.128) which include but are not limited to its planning; creation and organization; the receipt and capture of data; the retrieval, processing, dissemination and distribution of a *set of recorded information (SRI)*; its storage, maintenance and protection; its archival preservation or destruction or *expungement* (3.44)

3.136
SRI retention period
specified period of time that a *set(s) of recorded information (SRI(s))* (3.128) is kept by a *Person* (3.89) in order to meet operational, legal, regulatory, fiscal or other requirements

3.137
standard
documented agreement containing technical specifications or other precise criteria to be used consistently as *rules* (3.120), guidelines, or *definitions* (3.37) of *characteristics* (3.14), to ensure that materials, products, *processes* (3.100) and services are fit for their purpose

Note 1 to entry: This is the definition of standard in ISO and IEC (see also ISO/IEC Guide 2:2004, 1.7).

[SOURCE: ISO/IEC 15944-1:—, 3.64]

3.138
term
designation (3.38) of a defined concept in a *special language* (3.130) by a linguistic expression

Note 1 to entry: A term may consist of one or more words (simple term or complex term) or even contain symbols.

[SOURCE: ISO 1087-1:2000, 3.4.3]

3.139
third party
Person (3.89) besides the two primarily concerned in a *business transaction* (3.10) who is *agent* (3.2) of neither and who fulfils a specified *role* (3.119) or function as mutually agreed to by the two primary *Persons* or as a result of *external constraints* (3.45)

Note 1 to entry: It is understood that more than two Persons can at times be primary parties in a business transaction.

[SOURCE: ISO/IEC 15944-1:—, 3.65]

3.140
transitory record
set of recorded information (SRI) (3.128) that is required only for a very limited and specified (retention period) time to ensure the completion of a routine action or the preparation of a subsequent *set of recorded information (SRI)*

Note 1 to entry: A transitory SRI is expunged at the end of a short existence.

3.141
unambiguous
level of certainty and explicitness required in the completeness of the semantics of the *recorded information* (3.110) interchanged appropriate to the goal of a *business transaction* (3.10)

[SOURCE: ISO/IEC 15944-1:—, 3.66]

3.142
under the control of
set of requirements on an *organization* (3.86), especially those of *external constraint* (3.45) nature, i.e., *privacy protection* (3.97) and related *information law* (3.57) requirements, requiring full and complete *information life cycle management (ILCM)* (3.58) of *personal information* (3.90) as *set(s) of recorded information (SRIs)* (3.128) related to the agreed upon goal of the instantiated *business transaction* (3.10), including state changes to the content of the *SRIs* with respect to their creation/ collection, recording processing, organization, storage, use, retrieval, disclosure, retrieval, aggregation, dissemination, *disposition* (including *expungement* (3.44)), *electronic data interchange (EDI)* (3.41), etc., and in particular that of any and all state changes in the *decision making application (DMAs)* (3.35) of the *organization* and any of its *agents* (3.2) and/or *third parties* (3.139) (as well as any other parties) to the *business transaction*

Note 1 to entry: The fact that a Person responsible for the control of a SRI(s), especially SPI(s), delegates or contracts out physical custody of the SRI(s) to an agent or third party does not take away from the responsibility of that Person for ensuring ILCM management aspects in support of privacy protection requirements remain fully supported and executed.

Note 2 to entry: If and where a disposition or expungement of SPIs pertaining to a business transaction involves the transfer of the related SPIs to another organization the applicable ILCM requirements of a privacy protection nature continue to apply to the organization to which the SPIs are being transferred to.

3.143
vendor
seller (3.125) on whom *consumer protection* (3.26) requirements are applied as a set of *external constraints* (3.45) on a *business transaction* (3.10)

Note 1 to entry: Consumer protection is a set of explicitly defined rights and obligations applicable as external constraints on a business transaction.

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

[SOURCE: ISO/IEC 15944-1:—, 3.67]

3.144
vocabulary
terminological dictionary which contains *designations* (3.38) and *definitions* (3.37) for one or more specific subject fields

Note 1 to entry: The vocabulary may be monolingual, bilingual or multilingual.

[SOURCE: ISO 1087-1:2000, 3.7.2]

4 Abbreviated terms

ATI	access to information
BTM	business transaction model
cdRS	coded domain registration schema
CGSB	Canadian General Standards Board
CRPD	(UN) Convention on Rights of Persons with Disabilities
FOI	freedom of information
FTC	(USA) Federal Trade Commission
HTML	hypertext mark-up language
HTTP	hypertext transfer protocol
ICT	information communication technologies
IPD	information processing domain
NAFTA	North American Free Trade Agreement
OeDT	Open-edi descriptive techniques
OeR	Open-edi registry
OeRA	Open-edi registration authority
Oe-RRDS	Open-edi records retention and disposal schedule
OVN	open value network
PbD	privacy by design
PIPEDA	Personal Information Protection and Electronic Documents Act (Canada)
PPR	privacy protection requirement
pRS	persona registration schema
RAI	registration authority identifier
RRDS	records retention and disposal schedule
SI	semantic identifier
UML	unified modelling language (specified in ISO/IEC 19501 [25])

5 Fundamental privacy protection principles

5.1 Overview

This Clause is based on ISO/IEC 15944-8:2012, Clause 5. The rules found in ISO/IEC 15944-8:2012, Clause 5 are specified in Annex B.7. As such, this document shall meet the requirements of ISO/IEC 15944-8.

Rule 001:

The rules stated in Annex B of other parts of the ISO/IEC 15944 series, and in particular those of ISO/IEC 15944-8 (see Annex B.7), are relevant and shall be applied as specified in Annex B.

Rule 002:

"Aspects not currently addressed" as identified in ISO/IEC 15944-8:2012, 1.3 also apply to this document.

"Unambiguous" is an issue in business transactions because states of ambiguity and uncertainty are not desired from commercial, legal, consumer and information technology perspectives. Issues of unambiguousness apply to all aspects of a business transactions and even more so to those which are EDI-based. The need to support unambiguity facilitates requires international semantic interoperability among parties to a business transaction and thus the use of human interface equivalents (HIEs). In support of these eBusiness requirements, Annex A provides the HIEs in ISO English and ISO French language equivalents and does so in a matrix-based approach which facilitates it being extended to other HIEs for other languages (see ISO/IEC 15944-7 which provides the fundamental principles and rules for the development of a definition for a concept and the rules governing development of multilingual equivalents, i.e., as HIEs).

5.2 Primary sources of privacy protection principles

Figure 3 is taken from ISO/IEC 15944-8:2012, Figure 3. It is repeated to provide an overview of the sources of requirements of the privacy protection principles as they also apply to this document.

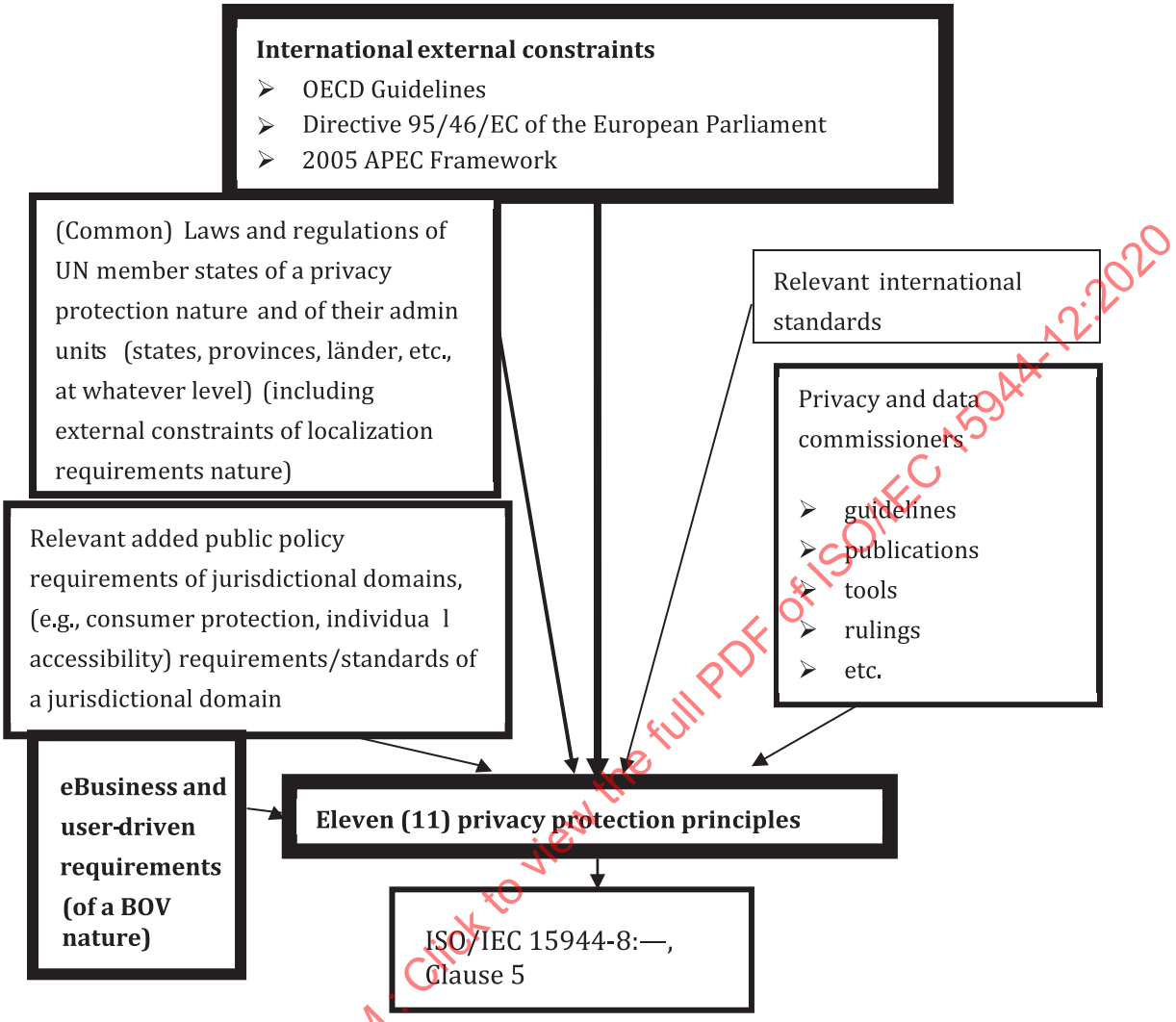

Figure 3 — Primary sources for privacy protection principles

5.3 Key eleven (11) privacy protection principles

Rule 003:

ISO/IEC 15944-8:2012, 5.3 provides eleven (11) principles, rules, guidelines and associated normative text. All apply to this document. They are:

- **Privacy protection principle 1: Preventing harm**
- **Privacy protection principle 2: Accountability**
- **Privacy protection principle 3: Identifying purposes**
- **Privacy protection principle 4: Informed consent**
- **Privacy protection principle 5: Limiting collection**
- **Privacy protection principle 6: Limiting use, disclosure and retention**
- **Privacy protection principle 7: Accuracy**

— **Privacy protection principle 8: Safeguards**

— **Privacy protection principle 9: Openness**

— **Privacy protection principle 10: Individual access**

— **Privacy protection principle 11: Challenging compliance**

These eleven (11) privacy protection principles are placed in a business transaction context, i.e., that of Persons, as parties, making a commitment on the commonly agreed upon goal for a business transaction.

From a FSV perspective, this includes ensuring that the IT systems of an organization are able to and do provide associated required technical implementation measures which need be capable of exchanging the necessary information among the parties to a business transaction. This is necessary to be able to determine when personal information is to be processed as opposed to all other (non-personal) recorded information forming part of the business transaction. This includes ensuring that applicable controls are in place in the decision-making applications (DMAs) of the IT systems of organizations (and public administrations) where personal information is processed and interchanged among all parties to a business transaction[9)].

Finally, the privacy protection principles enumerated above represent a whole and should be interpreted and implemented as a whole and not piecemeal. Implementers of this document should be aware that in subsequent clauses of this document, two or more of the privacy protection principles referenced may be instantiated together and simultaneously.

5.4 Link to "consumer protection" and "individual accessibility" requirements (see ISO/IEC 15944-8:2012, 6.3)

This document, as with ISO/IEC 15944-5 and ISO/IEC 15944-8, is based on the following assumptions:

1) The privacy protection requirements of the individual, as a buyer in a business transaction, are those of the jurisdictional domain in which the individual made the commitments associated with the instantiated business transaction. As such, this document shall be implemented in accordance with the requirements of ISO/IEC 15944-1 and ISO/IEC 15944-5;

2) Where the seller is in a jurisdictional domain other than that of the individual, as the buyer, this document incorporates and supports the:

   — *OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data*;

   — *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)*;[10)]

   — *APEC Privacy Framework. (2005)*;

   — *UN Convention on the Rights of Persons with Disabilities (CRPD) (2006+).*

3) Where the buyer is an "individual" this also incorporates individual accessibility requirements.

4) Where the buyer is an individual this also invokes consumer protection and individual accessibility requirements.

9) Relevant concepts and their definitions include: decision-making applications (DMAs), information processing domain (IPD), and Open-edi support infrastructure (OeSI) in IT systems, see ISO/IEC 14662:2010, 5.2 and Figure 3.

10) The "1995 Directive" is replaced by Regulation EU 2016/679. This Directive and associated rules applies from 25 May, 2018. EU member states transposed the new Directive into their national law by 6 May, 2018. It remains to be determined whether this reform of EU data protection rules introduces PPRs which are not already covered in the rules in this document.

In order to support ILCM implementation requirements in this document, it is important that these assumptions are explicitly stated, i.e., in the form of a rule.

Rule 004:

Laws and regulations governing privacy protection (as well as consumer protection and individual accessibility requirements) which apply where, in a business transaction. the buyer is an individual, are those of the jurisdictional domain of the buyer.[11)]

5.5 Privacy protection principles in the context of ILCM requirements

The purpose of this subclause is to supplement, from an ILCM perspective, the rules and associated text from each of the eleven privacy protection principles specified in ISO/IEC 15944-8:2012, 5.3.

Rule 005:

An individual, as a buyer in a business transaction, shall be able to challenge the timeliness and accuracy of his or her personal information including ILCM aspects including any state changes to the content value of such a set of personal information (SPI) as part of the ILCM of the organization in accordance with other applicable information law requirements, including retention, and expungement, as well as with respect to any ILCM management of a privacy protection requirements nature, in any use by the seller organization of an agent and/or third party to a business transaction.

Guideline 05G1:

An organization, in its role as seller or regulator, should provide its name, physical and electronic address and related contact information of its privacy protection officer (PPO).

5.6 Requirement for tagging (or labelling) sets of personal information (SPIs) in support of privacy protection requirements (PPR) in accordance with ISO/IEC 15944-8:2012, 5.4

The application of the general privacy protection principles, as stated in ISO/IEC 15944-8:2012, 5.3, requires an organization to be able to identify and tag any and all sets of personal information (SPIs) when created or collected in its IT systems. Such SPI-related tagging is required to enable an organization's compliance with specific privacy protection requirements, (e.g., via metadata or properties/actions assigned to cells in a database). An organization can do such tagging of sets of SPIs at the records level (e.g. client file level) down to the more granular data element level. For example, within an SPI there may be data elements to which PPR apply and data elements to which PPR does not apply. The same approach applies to state changes to an SRI, SPI and any data element within the same (see 8.4).

5.7 Requirements for making all personal information (PI) available to the buyer where the buyer is an individual

It is a best business practice, as well as a contractual obligation, for the seller to make available to the buyer, as an individual, all the personal information pertaining to the business transaction and to do so in a timely manner. Often organizations include access to tracking of the shipping of a project, updates on services, (e.g., travel, monthly statements, or provide real time online access) to the buyer/client to his/her business transaction information.

The focus of this document is on the personal information held by an organization on a buyer as an individual including not only the personal information of an instantiated business transaction but also and especially that of any SPIs independent of those pertaining to an instantiated business transaction and its associated business transaction identifier (BTI) (e.g. as a personal information profile).

11) This rule mirrors that of the EU requirement in online business transactions that apply sales taxes, (e.g., VAT) are those of the jurisdictional domain of the buyer.

Rule 006:

Upon request by an individual (as a buyer), the seller shall make available to that individual all personal information pertaining to that business transaction including associated metadata.

5.8 Rules governing ILCM aspects of personal information profiles (PIPs)[12)]

It is a common occurrence and business practice for a seller to establish and maintain a "profile" on its customers, i.e., in addition to or apart from the SPI resulting from an instantiated business transaction. It is understood that where the buyer is an individual, i.e., a customer, that:

a) the individual has consented to the organization, in the role of seller, retaining personal information on or about herself/himself;

b) the individual has provided the information to the organization including both "basic" personal information as well as that of the nature of personal preferences, etc., pertaining to the business transaction;

c) the organization preparing and retaining the "personal profile" has made clear to the individual detailed information, including those of RRDS nature, as to its use as well as choices with respect to further distribution or not of such personal information;

d) the right of the individual to update/change his/her PIP with the organization at any time including the "privacy controls", accessibility, "preference settings", etc.;

e) the right of the individual to request an organization with which it has established a personal information profile (PIP) for a copy of the complete set of recorded information at any time.

In a PPR context, there are 3–5+ common sources among jurisdictional domains for any organization to be able to collect/create and maintain sets of personal information on an individual:

a) as collected from publicly posted personal information services, [e.g., telephone directories, that are required to be made publicly available by public/governmental institutions (known as "publicly available information")];

b) as agreed to by the individual via expressed informed consent by the individual to be retained by the collecting organization (or shared with other secondary, tertiary organizations);

c) as created/collected by an organization as part of the identification and negotiation phase in a business transaction process which was not actualized but where the prospective buyer as an individual agreed that the seller could retain as part of its "customer information profile (CIP)";

d) as created/collected by an organization as part of the end of the negotiate phase leading into an agreed upon commitment to start the actualization phase;

e) as part of permitted state changes pertaining to a post-actualization phase of an instantiated business transaction.

There is also a need to differentiate between (a) SPIs pertaining to a buyer as an individual which pertain to an instantiated business transaction; and, (b) SPIs pertaining to a (prospective) buyer as an individual which the relevant seller organization maintains on an ongoing basis on that individual. This may apply even when no instantiated business transaction has occurred. Another example is where a seller may well invite an individual to agree to receive a catalogue or be kept informed, (e.g., via email) of product/service offerings by the seller on an ongoing basis. For example, a seller may invite a (prospective) customer to enrol in an "affinity" (points) programme even if the prospective customer has not (yet) engaged in an instantiated business transaction with that organization.

In support of these common practices of organizations (and public administrations) personal information profile (PIP) is defined in 3.92.

12) This is consistent with the overall approach of the ISO/IEC 15944 series starting with ISO/IEC 15944-1:—, 6.2.8.

Rule 007:

Before any Person, i.e., an organization or public administration, establishes a personal information profile (PIP) on or about an identifiable individual, it shall have: (a) the explicit and informed consent of that individual; and (b) have clearly identified and specified legal or regulatory requirements (of the applicable jurisdictional domain) which explicitly authorize the establishment of a PIP including the coverage or extent of the sets of personal information involved; or (c) a combination of (a) and (b).

Rule 008:

Any Person authorized to establish and maintain a personal information profile (PIP), as per Rule 007, shall ensure that applicable PPR information life cycle management (ILCM) requirements are identified and implemented, i.e., including those stated in this document.

A significant set of consumer protection requirements are similar in nature or complement privacy protection requirements. This was recognized in ISO/IEC 15944-1:—, 6.2.8 with regards to Person and external constraints for a consumer[13)] and vendor[14)]. As such, it is useful to introduce the concept and definition of consumer information profile (CIP) as defined in 3.25.

It is assumed that:

— any SRIs in a CIP can consist of one or more SPIs unless expressly designated as not containing any personal information (PI);

— on the whole, consumer protection requirements from an ILCM and EDI perspective are to be considered as supplementary or additional to (the more generic) privacy protection requirements.

Finally, it is understood that all SRIs comprising a consumer information profile are also sets of personal information. However, not all the SRIs or SPIs in a PIP are consumer specific/related.

6 Integrated set of information life cycle management (ILCM) principles in support of information law and privacy protection requirements (PPR)[15)]

6.1 Primary purpose of Clause 6

The primary purpose of Clause 6 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 have an information law component(s). These ILCM principles and their implementation are essential in order to ensure that any organization (or public administration) complies with ILCM related requirements which are embedded in their compliance with privacy protection requirements of applicable jurisdictional domains. 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 for the privacy protection principles presented in 5.3 and in particular, those which are required to be implemented in order to support PPR of applicable jurisdictional domains. The text and rules found in ISO/IEC 15944-8:2012, Annex D apply.

13) Basically a consumer is a buyer acting in the role of an individual (is an individual) and thus consumer protection requirements apply (see 3.24).

14) Basically, a vendor is a seller acting in the role of organization dealing with a buyer as a consumer and thus consumer protection requirements apply. Where a seller deals with a buyer who is an organization, this is commonly referred to as "B2B" and where a seller deals with a public organization, this is commonly referred to as "B2G" (G = government, i.e., public administration). Since for both B2B and B2G the buyer is not an individual, privacy protection requirements do not apply.

15) SPIs that are accurate, up-to-date and relevant with associated necessary ILCM policies and (auditable) procedures will likely not only be non-compliant with applicable privacy protection requirements but also all other applicable legal and regulatory requirements, and likely its fiduciary responsibilities.

Further, there are also legal requirements which pertain to any set of recorded information interchanged among parties to a business 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 procedures, documentation and related activities pertaining to business transactions and resulting sets of recorded information (SRIs) (consisting of one or more IBs or SCs) used in EDI require that the highest standards of integrity and trustworthiness are maintained. A primary factor is that business transactions represent the most common form of making and executing (legally binding) commitments among the parties concerned.

These information law requirements pertain not only to the flows of information and the contents of the recorded information but also to the many other existing laws, regulations, etc., impacting information management and EDI among persons, including supporting documentation. Examples of such laws impacting business 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.

From a high level perspective, and taking into account specific information law requirements of jurisdictional domains (as well as those pertaining to privacy protection requirements), one can group these ILCM requirements into a number of discrete categories.

Discrete categories of "information law" already identified with respect to personal information (PI) include those that:

— require one to keep or retain certain personal information;

— require one to track, note, any state changes to personal information;

— require one to have the ability to produce or retrieve certain types of personal information (see 7.4);

— require one to submit or file personal information to a government or regulatory agency;

— require one to create and/or make available personal information if one undertakes a particular activity, i.e., pertaining to a product, service and/or right;

— require one retain personal information "indefinitely" or for a specified period of time;

— require one to destroy, i.e., "expunge", personal information;

— place conditions on the manner in which one handles personal information;

— place conditions on the reproduction, distribution or sale of personal information; and

— place conditions on the sharing, linking or flows of personal information (within or among jurisdictions).

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.

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". 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 information communication technologies (ICT) has increased the need for trustworthiness, integrity, accountability, etc., which has made this "traditional" approach increasingly less viable.

The second approach is that of an integrated approach, which is more viable and practical. It is vital that an integrated approach to information life cycle management (ILCM) of the recorded information of an organization be approved and driven by senior management. It is also very important that such ILCM principles focus on the WHATs not the HOWs and be stated in simple, non-technical language (see 0.12).

The focus of Clause 6 is that of ILCM principles in support of enabling an organization to be able to comply with privacy protection requirements (PPR) applicable to personal information. It does so in the context of a business transaction where the (prospective) buyer is an individual and that most, if not all, of the sets of recorded information (SRI(s)) pertaining to that business transaction are sets of personal information (SPIs)[16].

6.2 Information life cycle management (ILCM) principles that support privacy protection requirements (PPR)

6.2.1 Compliance with privacy protection requirements (PPR) and associated information law requirements

Rule 009:

Where external constraints (of a relevant jurisdictional domain(s)), with respect to privacy protection requirements to a business transaction apply, the Person as a seller shall ensure that such privacy protection requirements (PPR) are identified and supported. This generic rule also applies to the identification of any and all ILCM related requirements[17].

These and related information law-based requirements are often quite similar in nature. It therefore benefits an organization to take an integrated approach to supporting and complying with information law requirements.

Guideline 009G1:

Any organization (for-profit or not-for-profit basis) (or public administration): (a) should have an accurate and up-to-date list of all information law requirements (ILCM) 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; (b) these need to include any and all applicable ILCM requirements; and (c) should be in full compliance with such information law requirements.

Guideline 009G2:

In support of the implementation of this rule, an organization should have in place a systematic and IT-enabled record retention and disposal schedule (RRDS) which applies with and implements PPR as well as other information law requirements (see 8.6).

6.2.2 Direct relevance, informed consent and openness

Rule 010:

Any personal information (PI) which exists within an organization pertaining to a (potential) buyer in a business transaction shall be directly relatable and relevant to the (agreed upon) goal of the business transaction, including applicable ILCM requirement, as well as being able to support applicable PPR.

16) It is up to users and implementers to decide whether or not to extend privacy protection ILCM requirements to other types of SRIs under the control of their organization and/or in their EDI, e.g., with respect to SRIs interchanged as IBs and their SCs with respect to business transactions of a "B2B" (business-to-business) or "B2G" (business-to-government/ government-to-business) nature.

17) Annex B.7 provides a consolidated list of rules found in ISO/IEC 15944-8 which identify external constraints of relevance to supporting privacy protection requirements. Further, ISO/IEC 15944-8:2012, Clause 7 identifies a number of other public policy requirements of jurisdictional domains which apply where and when the Person in the role of a buyer in a business transaction is an "individual". These include "consumer protection", and "individual accessibility".

Privacy protection requirements include the need that only personal information that one collects or creates which is directly related to the goal of the business transaction may be retained.

As to what is personal information of direct relevance to a business transaction, this is determined by the goal of the business transaction.

Each business transaction pertains to a specific and specified goal which the parties to the transaction have committed themselves.

This clause and its rules complement those of ISO/IEC 15944-8:2012, 5.3.3, which are applicable.

Rule 011:

In specifying the goal of a business transaction, the organization collecting or creating the personal information shall also identify and specify applicable ILCM aspects and inform the individual accordingly.

It is very important in a business transaction (or any form of commitment exchange) that where the buyer is an individual, that individual is fully informed on any and all ILCM aspects related to the personal information created or collected as part of that business transaction. For example, the personal information pertaining to the business transaction will be kept for two years after the transaction is completed after which it will be expunged.

The records retention period for the set of personal information (SPI) depends on the type of business transaction and the applicable laws in the jurisdictional domain, e.g., all finance records are kept for 6–7 years. There is thus a link to the organization's records retention schedule, which in turn supports applicable laws/regulations in the jurisdictional domain. The personal information may have to be retained, for example, if the purpose for which it was collected is still valid, i.e., it has to meet legislation. If the finance/tax laws do not require the retention of personal information, then there is another task: to delete all personal information but keep the rest of the record for tax purposes. Logistics of an ILCM nature in support of the same are required to be specified in rules/guidelines which in turn are required to be linked to RRDS.

Rule 012:

As part of the identifying purpose, the seller shall state to the potential buyer, when this is an individual, whether personal information collected on or received from that individual will be expunged or retained for a specified time period, should the intended business transaction not be actualized (see 8.6).

Rule 013:

The default rule in support of Rule 008 is that, if the individual does not provide explicit informed consent, that such personal information be expunged by the seller as soon as possible, as permitted by applicable information law requirements.

Rule 014:

As part of identifying purpose, the organization collecting or creating the personal information in the context of the specified business transaction shall state to the buyer whether or not such personal information will be shared, (e.g., via EDI) with other organizations and, if so, only with those organizations which in their operations support privacy protection requirements.

Rule 015:

The default rule is that the individual (as the prospective buyer) needs to (a) be formally/explicitly requested to provide his/her informed consent to the seller (organization) to share her/his personal information with other organizations; and (b) be informed of which explicitly stated ILCM and "under the control of" conditions exist with any and all other organizations.

The principle of "informed consent" requires that the individual, as prospective buyer, be fully and explicitly informed by the seller 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. This principle is clearly a requirement to flag personal information, i.e. any SPI, supplied as being for limited use.

Rule 016:

The principle of informed consent applies to any and all ILCM aspects of the personal information created or collected as may be required, especially that of keeping a record of such an informed consent and being able to produce it as evidence of the same.

Guideline 016G1:

Organizations should have and make available to prospective buyers, i.e., as individuals, the organization's ILCM policy as it applies to the personal information forming part of the business transaction.

The principle of "openness" pertains to the privacy protection requirement that any organization which collect and uses personal information shall be fully transparent in its use of personal information. This means that all of its policies and business 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. This also applies to those of an ILCM nature. This clause and its rules complement those of ISO/IEC 15944-8:2012, 5.3.9, which are applicable.

Rule 017:

An organization shall have and make available to any individual, as a buyer in a business transaction, specific information about its policies and practices of an ILCM nature including state changes, retention periods, disposal, etc., including how these are enforced with respect to the use of agents and/or third parties to the business transaction.

Guideline 017G1:

An organization can do so on a case by case basis. However, a systematic approach, which is recommended, would be the development and maintenance of a record retention and disposal schedule (RRDS).

6.2.3 Ensuring that personal information is "under the control of" the organization throughout its ILCM

Rule 018:

An organization shall ensure that any personal information (PI) pertaining to a business transaction remains completely "under the control of" that organization (at all times) including any EDI as well as the use an PI by agents and/or third parties in support of any phase of the process component of the business transaction.

Guideline 018G1:

In order for an organization to be able to support business transaction audit trail requirements, from both internal constraints (e.g., fiduciary, operational) and external constraints, an organization should ensure that all its recorded information remains under its control.

It is noted that even if the particular business transaction is not actualized, the individual prospective buyer, i.e., as consumer, may give informed consent to his/her personal information profile (PIP) being retained by the (prospective) seller organization.

Clause 7 expands on this fundamental ILCM principle of "under the control of" in a privacy protection requirements context.

6.2.4 Limiting use, disclosure and retention

This subclause and its rules complement those of ISO/IEC 15944-8:2012, 5.3.6, which apply here. Further, 8.6 provides the added rules necessary for systematic and IT enabled approach to "limiting retention" of personal information.

Rule 019:

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

From an ILCM perspective, this principle is particularly relevant and important especially that the requirement on an organization to limit the retention of personal information pertaining to a business transaction be supported in the IT systems of that organization.

Rule 020:

Unless expressly required to be retained due to external constraints of the applicable jurisdictional domain(s), or directly linked to the purpose and nature of the business transaction, all personal information (PI) collected, created or received pertaining to the planning, initialization and/or negotiation of a business transaction shall be expunged when the business transaction is not actualized.

Rule 021:

The seller in a business transaction shall ensure that any and all use within an organization of any PI shall be limited to the purpose of the business transaction.

Guideline 021G1:

It is advised that personal information pertaining to (the same type of) business transaction be managed within a specified DMA(s) to facilitate implementation of required functional support services.

Rule 022:

Personal information shall be retained by the seller only for as long as is necessary for the fulfilment of those purposes as specified as part of the business transaction.

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

Personal information is required to 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.

Rule 023:

Organizations 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 business transaction shall be destroyed (expunged) by the organization or its agents where applicable, and in a manner which can be verified via audit procedures.

Guideline 023G1:

For most, if not all, instantiated business transactions, external constraints of the applicable jurisdictional domain(s) require that specific sets of recorded information (SRIs) pertaining to any business transaction be retained by the seller for a specified period of time and then disposed of, including their expungement.

It is recognized that, depending on the nature of the good, service and/or right which is the goal of the business 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 business transaction.

It is also recognized that where the purchase of a 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 business transaction. A primary example of an internal constraint nature is that of a "warranty" for "n" number of years[18]. This includes the possibility that the individual who made the purchase may not be the "warranty holder".

EXAMPLE Where the good or service is purchased as a gift, 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.

The following rules summarize these requirements from a BOV perspective:

Rule 024:

The seller shall identify to the buyer, especially where the buyer is an individual, any and all record retention and disposal requirements pertaining the resulting SRIs, and in particular any SPIs forming part of the specified goal of a business transaction as a result of applicable external constraints of jurisdictional domain(s) as a result of the actualization of the business transaction.

Guideline 024G1:

The seller organization should incorporate all record retention and disposal requirements into the management of its business transaction audit trail in order to be facilitate its compliance with privacy protection transactional integrity requirements.

Rule 025:

Where the seller offers a warranty, or extended warranty, as part of the business transaction, the seller shall inform the buyer, when the buyer is an individual, of the associated added records retention and disposal requirements for the sets of personal information (SPIs) associated with the warranty (including the purchase by the individual of an extended warranty).

The sale of many types of goods or services require the seller to inform the buyer 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.

Rule 026:

Where the buyer in a business transaction is an individual, the seller shall inform the individual of any and all records retention and disposal requirements of sets of personal information (SPIs) which is recorded as the result of the actualization of the business transaction, including:

1) **personal information which is required to actualize the business 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**

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

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 business transaction.

From a customer service perspective, many sellers, i.e. organizations (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, as well as obtaining client feedback, surveys, new product announcements, etc.

Rule 027:

Where the buyer in business transaction is an individual, the seller shall inform that individual of the applicable record retention conditions where these pertain to personal information.

It is important when the buyer is an individual that, prior to and at the actualization phase in a business transaction, the individual is fully informed by the seller of its records retention and disposal requirements and practices of the seller 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 business transaction, that certain types of personal information may be subject to differing records retention periods.

It is noted that where the business transaction is one of the nature of the provision of a service or a right (such as a license or authority of some kind) the seller needs to retains a specified set(s) of personal information for as long as a business transaction of this nature remains active.

Rule 028:

Where a business transaction does not reach the actualization phase, any personal information collected by the organization in support of that transaction shall be deleted, i.e. expunged, by the organization (unless the individual concerned explicitly consents to the retention of such personal information for a defined period of time by that organization).

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

It is noted that this rule makes provision for the possibility that the individual, as a prospective buyer, may consent to be kept informed by the seller about product information via a catalogue, special sales, new offerings, etc. Such a decision by the individual is of the nature of obtaining "informed consent".

Particular care needs to 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, for a purchase and payment, it may not be necessary for the seller to know the actual personal identity of the buyer. The seller may need only to have an identifier by which that buyer may be uniquely identified to the seller. It may be sufficient that the seller is certain of payment because the seller 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 buyer and seller in order to fulfil its requirements in the transaction (but not the content of the transaction), whilst the seller does not need to know the identity of the buyer. 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).

6.2.5 Timely, accurate, relevant

NOTE This sublause and its rules complement those of ISO/IEC 15944-8:2012, 5.3.1 and 5.3.7, which apply here.

Rule 029:

All personal information pertaining to a business transaction shall be timely, accurate and directly relevant to the goal of the business transaction.

Rule 030:

Where the organization needs to share personal information pertaining to a specified business transaction (e.g., via EDI), such personal information shared shall also be limited to that which is absolutely necessary and relevant.

Most often the EDI aspects pertain to a limited sub-set of the personal information pertaining to a business transaction.

Rule 031:

Any personal information which is not accurate, timely or relevant shall not be entered or, if entered, shall be expunged immediately from (all the DMAs in) the IT system of the Open-edi party, and the DMAs in all the IT system of all the Persons with which the Open-edi party shared such personal information.

Guideline 031G1:

Any personal information of the nature identified in Rule 029 should be expunged immediately or at the minimum no later than as part of the ILCM update cycle of the relevant DMA (or IT system) of the seller (and its agents as well as any third parties associated with the instantiation of the business transaction).

It is vital that Persons do not collect or retain any personal information which may harm an individual. This applies especially where such personal information is not accurate, timely and/or relevant to the business transaction.

It is to the mutual benefit of all parties to a business transaction, and also a good business practice, to ensure that any and all recorded information pertaining to a business transaction be as timely, accurate, complete, up-to-date, etc., as possible. Accuracy of recorded information is an essential component of "integrity" which is a major asset of any organization. Organization should not keep recorded information on its business transaction or its clients which is not accurate or out-of-date, especially in the DMAs of its IT systems. Organizations concluding business transactions with buyers, as individuals, should have no difficulties in supporting the external constraint of "accuracy" of a privacy protection nature (including in the DMAs of their IT systems).

An organization which does not have policies and auditable procedures in place as part of its overall governance should ensure that the recorded information on which its decisions and commitments are made be documented and publicly available with respect to its privacy protection policy and associated ILCM policies and procedures.

The privacy protection "accuracy" principle is closely related to ensuring the "SRI integrity" in an ILCM context, i.e., the trustworthiness of personal information throughout its life cycle [including, where applicable, personal protection transactional integrity (PPTI)].

Rule 032:

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 business transaction.

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 practice. For a variety of reasons, organization 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 032G1:

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

Guideline 032G2:

It is recommended that the organization make available such ILCM information at the planning phase or, if not, during the identification phase and no later than the negotiation phase of the business transaction.

6.2.6 Data integrity and quality

Rule 033:

Information management policies and practices, including those of an ILCM nature, as well as those of supporting information handling systems for personal information shall ensure that the level of trustworthiness, data integrity, i.e., SRI integrity, quality and dependability for such personal information supports applicable privacy protection requirements.

It is to the mutual interest of the two primary parties to a business transaction, i.e., the seller and the buyer, to ensure and maintain a "100 %" level of data integrity and quality with respect to the SRIs pertaining to any instantiated business transaction. Privacy protection requirements serve as a set of external constraints to ensure the data integrity and quality of a SIR pertaining to the business transaction and especially any sets of personal information (SPIs) forming part of the (prospective) business transaction.

6.2.7 Safeguards for non-authorized disclosure requirements

This principle also introduces the concept of protection. Protection involves one or more constraints that are to be applied to specific data which 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 type of privacy protection that is to be provided, but that it is for the FSV implementation to determine how such privacy protection requirements are given technical effect. In this document only the means of determining the agreed (or required) privacy protection that is attaching to specified SRIs (data elements fields, records, etc.) is addressed.

NOTE This subclause and its rules complement those of ISO/IEC 15944-8:2012, 5.3.7, which applies here.

Rule 034:

Where required (or warranted), personal information should be protected from premature and/or non-authorized disclosure. Adequate safeguards shall be enacted to ensure the required levels of privacy protection within the seller organization (and its EDI parties).

It is important to note that the corollary of this ILCM principle, i.e., mandated disclosure, is supported equally. That is, recorded information, which the public in general and/or specified Persons have a right of access to, should not be withheld from disclosure.

Rule 035:

Personal information shall be protected by operational procedures 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, including such measures as are appropriate to ensure that all applicable legal requirements are supported.

Guideline 035G1

The organization should have in place the specified role/function of a privacy protection officer (PPO) who is responsible for ensuring that organization-wide policies and operation procedures are in place to support the same.

Guideline 035G2:

The organization should have in place the specified role/function of personal information controller (PIC) who is responsible for ensuring that, with respect to any instantiation of a business transaction of the organization, all the privacy protection requirements are implemented and in particular all of those of an ILCM nature.

Rule 036:

To support the "safeguard" principle in an ILCM requirements context, an organization shall ensure that no personal information, i.e., including any state change to the content value of a SRI, is destroyed, altered, falsified, rendered meaningless or useless, etc., by non-authorized means thereby ensuring the continued integrity and authenticity of any and all SRIs, IBs, and SCs pertaining to a business transaction.

Guideline 036G1:

Where an organization 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.

Rule 037:

With respect to implementing Rule 036, rules found in 6.2.8 apply.

6.2.8 Back-up, retention and archiving

It is recognized that prudent administration of data within an organization involves the systematic creation of back-up copy(ies) of data in whole or in part of SRIs contained in its IT systems. Back-up copies of data and their retention (including SPIs) are developed and maintained:

— in support of ILCM requirements as a whole;

— for those specific to a business transaction (including associated applicable external constraints); and/or,

— for those required for archival purposes;

— for historical, statistical and/or research purposes (see 6.2.11).

Rule 038:

Organizations shall ensure adequate back-up and contingency planning for any and all sets of personal information (SPIs) pertaining to a business transaction.

Rule 039:

Organizations shall retain any and all set(s) of personal information (SPIs) at the required level of detail as required by applicable information law and/or post actualization requirements (e.g., in relation to a warranty) and, in particular, in support of applicable privacy protection requirements.

Rule 040:

Any set of personal information (SPI) which has long-term value, i.e., forms part of the corporate memory and/or for historical, archival and/or research value should be identified and conserved. This includes SPIs information required for contingency planning, back-up, emergency response and related requirements.

Rule 041:

Where the buyer is an individual, personal information shall be considered confidential among the parties to the business transaction and not disclosed to any other party unless: (a) so permitted or authorized under applicable privacy protection legislation and regulation; or (b) with the explicit and informed consent of the individual whose personal information it is.

6.2.9 Disposition and expungement

Rule 042:

Any personal information which is no longer relevant to an organization's operations and which does not meet the above criteria should be disposed of immediately, i.e., in accordance with the organization's ILCM policy and practices, which in turn shall be privacy protection requirements-compliant. This includes any personal information whose ILCM properties from part of the business transaction.

Rule 043:

The disposition and expungement of any and all sets of personal information (SPIs) shall use and be done in accordance with rule 040 and associated (more) detailed rules as provided in this document.

6.2.10 Organizational archiving

Rule 044:

Where a business transaction involves personal information, the Open-edi records retention and disposal schedule (Oe-RRDS) period shall be established by the (seller) organization prior to the actualization of the business transaction.

Guideline 044G1:

It is advised that with respect to any good, service and/or right which is the goal of business transactions offered, that the seller (organization) prepares and makes available the information and the associated Oe-RRDS to prospective individuals as buyers.

Guideline 044G2:

It is also advised that with respect to any business transaction, and particularly those where the buyer is an individual, there be a link between the Oe-RRDS process and the business transaction identifier(BTI) in order to ensure efficient and systematic application of the Oe-RRDS and in support of meeting applicable privacy protection requirements.

Organizations (and public administrations) can group or categorize their Oe-RRDSs generally or by categories of their (offered) business transactions. For cost-effective and efficient conduct of their business activities, organizations also have in place Oe-RRDS which are cost-effective, efficient and implemented in a very systematic manner.

6.2.11 Historical, statistical and/or research value

It is a common practice, as well as one sanctioned and supported through relevant applicable information law, that personal information collected or provided as SPIs for a specific purpose in support of particular decision-taking and commitment-making pertaining to the individual, i.e., in any

type of business transaction, is and can be used for other purposes where so permitted or sanctioned based on applicable information law (and pursuant regulations and related legal instruments). This is especially so with respect to SPIs provided to or collected by public administrations use in a business transaction.

Rule 045:

Personal information which has historical value should be identified and conserved (as part of the organization's and/or electronic cultural heritage ("patrimoine informatisée").

It is not uncommon that personal information resulting from a business transaction may have historical or research value. This is especially so in public organizations and governments. For example, many jurisdictional domains have archiving legislation which allows their archives to retain non-active personal information. However, the archiving of such personal information is often accompanied by protocols restricted access to and use of such personal information. The same situation is common in medical institutions.

Rule 046:

Applicable archival or research-oriented legislation or regulation may exempt specified personal information from being expunged.

It is noted that research-oriented legislation, as well as (international) research protocols usually require that personal information to be used with respect to (longitudinal) research projects be anonymized. In addition, personal information which is retained for archival purposes may only become publicly available after the death of the individual, after 100 years, or according to legislative or regulatory constraints which are similar in nature.

Rule 047:

As part of his explicit and informed consent in entering into a business transaction, an individual may request or agree to allow the party in the role of seller to retain specified personal information after normal or statutory retention period has expired.

Rule 048:

Where the buyer in a business transaction is an individual, the seller shall provide detailed information on the seller's retention and disposal schedule for personal information created or collected during any of the five phases of the business transaction.

Apart from the fact that privacy protection requirements apply to the seller with respect to retention and disposal of any and all personal information pertaining to the prospective individual buyer, depending on the nature of the business transaction, various legal, regulatory, statutory, etc., records retention and disposal authorities apply. For example, the financial aspects of a business transaction may be required to be retained for a minimum of seven (7) years following the completion of a business transaction. Also, certain types of personal information may be required to be retained "forever". Many of these involve information law requirements of a generic nature and are usually maintained by public administrations or their agents, (notaries, lawyers, etc.). Examples include titles of property (sale records), marriage (and divorce) records, etc.

Rule 049:

Any personal information which would have been expunged in the normal and ordinary course of the business transaction in compliance with applicable ILCM and privacy protection requirements, but which was not expunged because it is to be used for research or historical purposes, shall be anonymized in any of its research use until such time as privacy protection ceases to apply to the such sets of personal information (SPIs).

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

The application of the general privacy protection principles, as stated in ISO/IEC 15944-8:2012, 5.3, requires an organization 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 to enable an organization's compliance with specific privacy protection requirements, (e.g., via metadata or properties/actions assigned to cells in a database). An organization can do such tagging of sets of recorded information at the records level (e.g. client file level) down to the more granular data element level.

Rule 050:

An organization shall have in place policies and procedures in order to identify and tag (or label) all sets of recorded information (SRIs) which contain personal information (e.g., as SPIs), i.e., where the buyer to a business transaction is an individual, and to do so at the appropriate level of granularity to facilitate compliance with both generic and specific privacy protection requirements. This includes any labelling needed to support implementation of any and all ILCM requirements.

Rule 051:

Where necessary to comply with ILCM requirements, the organization shall add tags to SRIs required to support the execution and management of state changes, retention periods, disposition, etc.

7 Rules governing ensuring accountability for and control of personal information (PI)

7.1 Purpose

This document shall conform to Open-edi reference model specified in ISO/IEC 14662.

The purpose of this Clause is:

— to support key characteristics of Open-edi;

— to introduce in summary form, key aspects and requirements of "under the control of"; and

— to do so in the context of privacy protection requirements generally and that of associated information life cycle management requirements specifically.

7.2 Key aspects of Open-edi requirements

A key and very relevant characteristic of Open-edi is that "parties control and maintain their states", as specified in ISO/IEC 15944-1:—, 5.4.

This Open-edi requirement is very relevant when and wherever the buyer in a business transaction is an individual and therefore requirements of a privacy protection nature apply (see ISO/IEC 15944-1:—, Clause 5). Further, as a business transaction involves the making of a commitment(s) among parties to a business transaction, the ISO/IEC 14662 Open-edi reference model introduced the concept and definition of decision-making application (DMA) which is where all set(s) of recorded information and associated state changes of a SRI are managed and controlled, including their EDI through information bundles (IBs) and their semantic components (SCs) with all parties to the business transaction. This Open-edi approach is especially relevant and applicable in the context of ILCM aspects in support of privacy protection requirements.

7.3 Key aspects of "under the control of"

The phrase "under the control of" is used in several international conventions and laws, as well as those of jurisdictional domains of UN member states. Included are related concepts of "held by", "in possession of", "controls", "in the care of" (i.e., "custody"), etc. The concept of "under the control of" with respect to sets of recorded information of an organization is widely used, including at all levels of jurisdictional domains, and is found most often within information law (and associated regulatory) requirements. The concept itself is not well-defined.

The legal and regulatory requirements of various levels of jurisdictional domains use other phrases to convey similar and/or parallel intent to include varying degrees of "control" and "custody". These phrases include:

— held by;

— responsibility of;

— in the possession of;

— in the custody off;

— maintained by;

— maintain and manage;

— in the care of.

7.4 "under the control of" in support of PPR and in an ILCM context

The requirements and rules in ISO/IEC 15944-8:2012, 5.4 apply to this subclause.

Existing Open-edi and eBusiness concepts and their definitions which are integrated into the definition for the concept of "under the control of" (see 3.144) include:

— agent;

— business transaction;

— decision-making application (DMA);

— electronic data interchange (EDI);

— external constraint;

— information law;

— information life cycle management (ILCM);

— organization;

— organization Person;

— personal information;

— privacy protection;

— set of recoded information (SRI);

— third party.

Information life cycle management (ILCM) pertains to all stages of a set of recorded information (SRI) from its initial creation/collection, processing and use (including EDI) to its eventual disposition. What privacy protection requirements (PPR) add to this is that all parties to a business transaction shall

maintain the same high level of "under the control of" and associated state changes with respect to personal information interchanges with both the individual and any other parties to the business transaction, (e.g., via EDI). Consequently, "under the control of" is defined as in 3.142.[19)]

Rule 052:

The organization which is the primary party to a business transaction, i.e., the seller, shall ensure that it establishes and retains "control" of all personal information pertaining to a business transaction, including where such personal information (PI) and/or set of personal information (SPI) is shared with an agent or third party (e.g., via EDI).

The fact that a Person as seller – and as such responsible for the control of a SRI(s), especially SPI(s) related to a business transaction or a personal information profile (PIP) – delegates out or contracts out physical custody of the SRI(s) to be processed, which are managed by the IT system of an agent or third party, does not take away the responsibility of that Person for ensuring that such a SRI(s) and in particular SPI(s) remains under the control of that Person.

Rule 053:

Before a seller in a business transaction, where the buyer is an individual and thus involves personal information, uses an agent or third party for any part of the processes and EDI pertaining to the business transaction, the seller shall ensure that an agent or third party has in place controls in the governance of its IT systems in support of privacy protection requirements (PPR) in compliance with Open-edi standards and related ILCM requirements.

A key responsibility of a privacy protection officer is to ensure that the organization shall not permit the EDI of any personal information outside the jurisdictional domain of an individual as buyer in a business transaction without assurance and demonstrated proof that the jurisdictional domain(s) to which such personal information is being interchanged (e.g., via EDI) has equivalent legal/regulatory privacy protection requirements.

Basically, an individual as buyer in a business transaction has privacy protection requirements based on those of his/her jurisdictional domain. The seller, as an organization or public administration, can decide to "outsource" any of its IT system support activities (as permitted by applicable information law), which would take place via EDI, to anywhere in the world as long as the jurisdictional domain in which such information processing, storage, etc., takes place provides privacy protection requirements equivalent to those of the jurisdictional domain of that individual.

7.5 Implementing "under the control of" and accountability

This clause and its rules complement those of ISO/IEC 15944-8:2012, 5.3.2 which applies.

While the role of PPO focuses on responsibility for corporate governance compliance with applicable PPR, the role of the personal information controller(s) (PIC) focuses on responsibilities pertaining to the implementation of the related ILCM requirements. On the whole, in (large) organizations, a PPO has organization-wide responsibility while those of a PIC may pertain to one or more DMAs in the IT system(s) of the organization, or that of a specified organizational unit. In smaller organizations, the roles of a PPO and PIC may well be carried out by a single organizational Person.

ISO/IEC 15944-8 introduced the concept and definition of a privacy protection officer (PPO) (see ISO/IEC 15944-8:2012, 5.3.2). In an Open-edi reference model context, the focus of the privacy protection officer (PPO) is primarily one of governance from a business operational view (BOV) perspective. The definition in ISO/IEC 15944-8 for the concept of privacy protection officer is given in 3.98.

Figure 4 illustrates the role of a privacy protection officer based on ISO/IEC 15944-8.

19) This definition integrates key aspects of "under the control of" as found in the APEC Privacy Framework as well as the Directive 95/46/EC on "data protection". The new EC "GDPR" has replaced the 1995 Directive. However, the essential "under the control of" requirements have not changed.

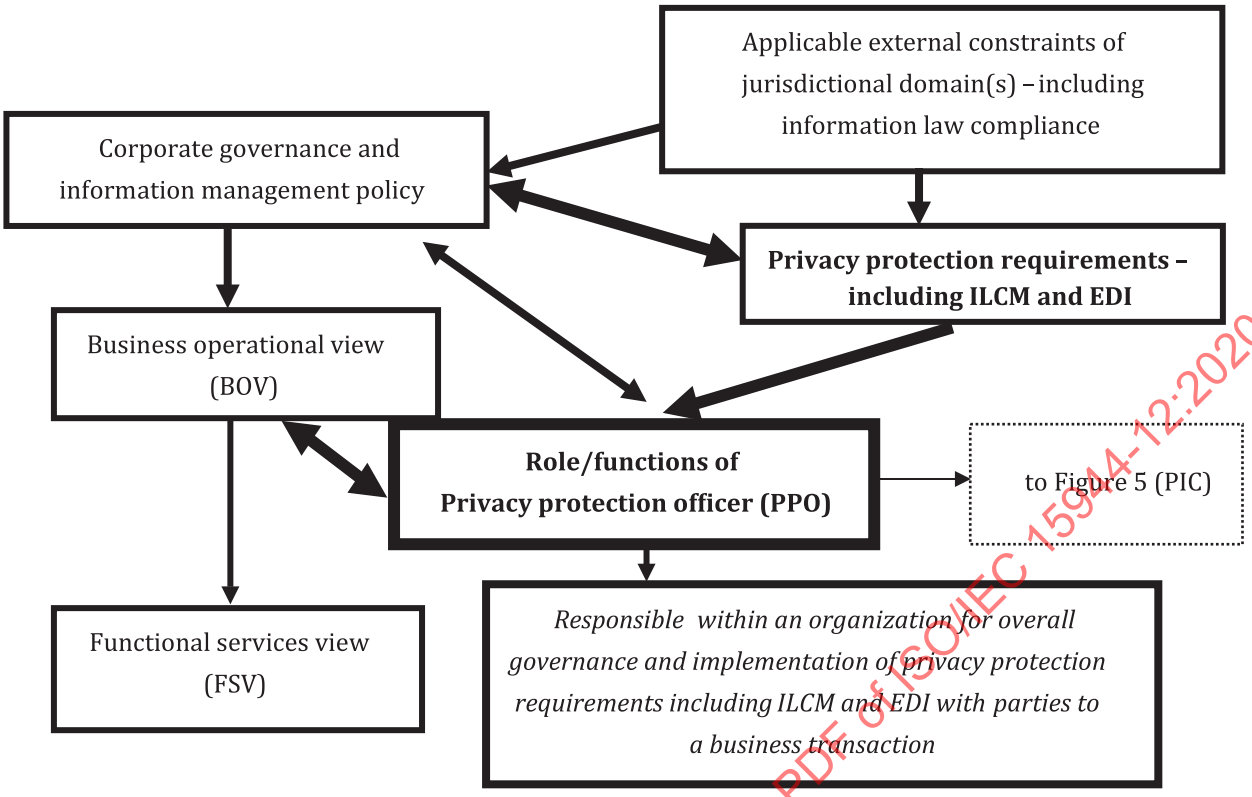

Figure 4 — Role of a privacy protection officer (PPO) based on ISO/IEC 15944-8 in an ILCM and Open-edi context

The role and responsibilities of a privacy protection officer (PPO) are of an organization-wide nature, related to ensuring that corporate governance complies with and supports applicable privacy protection requirements. However, ensuring that privacy protection requirements are actually implemented requires management and (detailed) control at the operational level.

The information life cycle management (ILCM) of this document is more focused on implementation aspects as well as serving as a bridge between the BOV and FSV. Whether or not the seller organization is a small or large organization, it needs to have a designated director, manager, etc., in charge of ensuring that at the day-to-day operational and ICT technical level privacy protection requirements are implemented. This is the role and function of a personal information controller in an organization. This role and function in an organization of a PIC is defined in 3.91[20)].

Figure 5 illustrates the role and function of a privacy information controller (PIC) in an organization in an Open-edi context.

20) This definition draws heavily on and is harmonized with the concept and definition of "data controller" as found in the Directive 95/46/EC on "data protection" of the European Union.

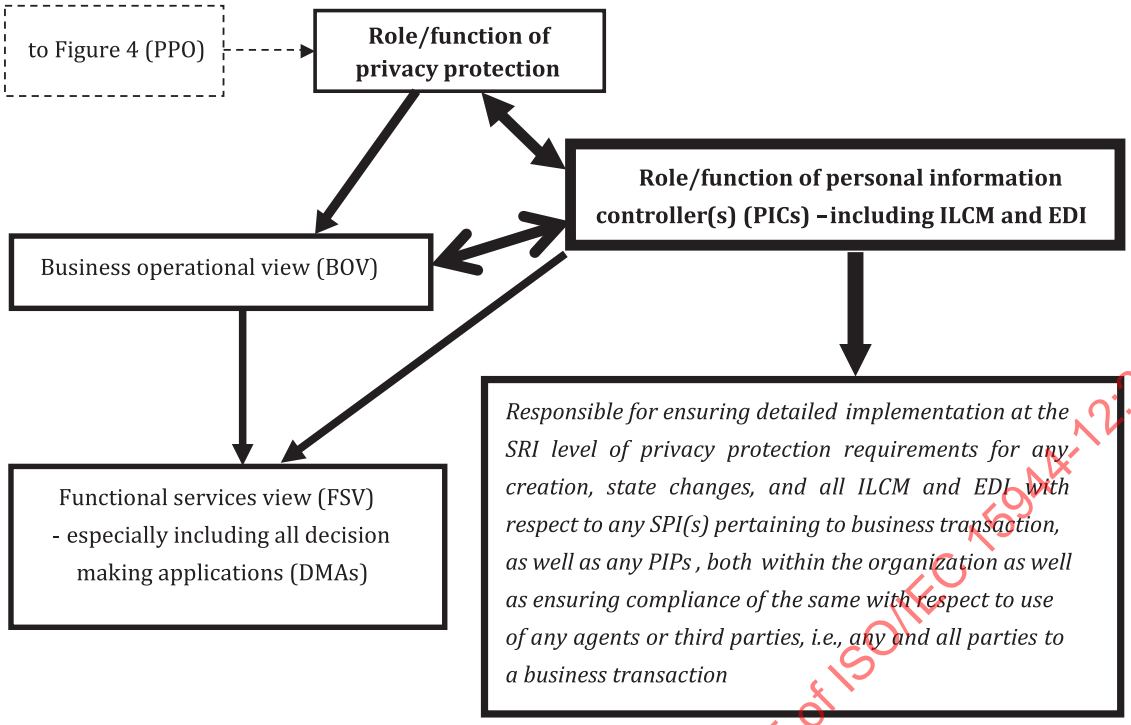

Figure 5 — Role, responsibilities and relationship of a personal information controller (PIC) in an organization in Open-edi context

Rule 054:

An organization shall ensure that it has a designated role and function of personal information controller (PIC), i.e., an organization Person who is responsible for ensuring that all processing, state changes, EDI, etc., of set(s) of personal information (SRIs) pertaining to a business transaction remain under the control of the organization, i.e., in its role as a seller.

Guideline 054G1:

It is also recommended that from a data processing and EDI perspective, that the organization has its personal information controller (PIC):

a) ***review any (prospective) EDI of the (seller) organization of any SPIs, as well as any state changes to the contents (and/or metadata on the same); and***

b) ***ensure that such SPIs remain under the control of the (seller) organization at all times, and in compliance with the ILCM requirements which apply to the SPIs of the business transaction including those of the IT system(s) of agents and/or third parties who may be involved.***

Guideline 054G2:

Where the organization is large, it may benefit from having a PIC for each of its DMAs which involve personal information[21)]***.***

Rule 055:

An organization should ensure that its privacy protection officer (PPO) has direct liaison with the (senior) officer(s) in that organization responsible for ILCM related aspects for any and all SRIs maintained by the organization and in particular the organization's personal information controller (PIC).

21) The assignment of PICs can be linked to each IT system where an organization has multiple IT systems, etc.

It is up to each organization to decide how to assign responsibility for ILCM, i.e., among records managers, archiving, information managers, IT managers, security managers, etc. However, in order to ensure that legal and regulatory requirements applicable to personal information in an IT system of that organization are implemented, it is vital that the PPO of that organization is given the mandate on an organization-wide basis, to be able to ensure that there is a very clear and transparent organization policy and process able to ensure and support full compliance with applicable ILCM aspects of privacy protection requirements.

Rule 056:

Where an organization interchanges personal information (e.g., through EDI) with one or more other organizations, i.e., as via its agent(s) and/or third party(ies), it shall ensure (e.g. its privacy protection officer (PPO)) that the other organization in their operations and IT systems support privacy protection requirements.

Guideline 056G1:

It is recommended from a legal, risk management and business best practices perspective, that an organization request its privacy protection officer (PPO), to review any (prospective) EDI of the (seller) organization of any SPIs pertaining to a (prospective) business transaction with any (potential) agent and/or third party, to ensure that any such Open-edi parties have in place in their IT systems the ability to support applicable privacy protection requirements, and are willing to sign a contractual arrangement in support of the same (e.g., of the nature of conformance statement provided in Clause 11).

The organization acting in the role of "seller" (or "regulator) has an obligation to ensure that privacy protection requirements are applied to personal information. This applies especially where the organization interchanges such personal information with another organization (as per informed consent of the individual for that business transaction).

Guideline 056G2:

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

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

It is also recognized that where the purchase of a good, service and/or right involves "post-actualization" aspects of a temporal nature, these will also impact record retention requirements and obligations resulting from an actualized business transaction. A primary example of an internal constraint nature is that of a "warranty" for "n" number of years[22]. This includes the possibility that the individual who made the purchase may not be the "warranty holder".

EXAMPLE Where the good or service is purchased as a gift, 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.

The following rules summarize these requirements from a BOV perspective:

Rule 057:

Where the seller offers a warranty or extended warranty as part of the business transaction, the seller shall inform the buyer, when the buyer is an individual, of the associated added records retention requirements for the personal information associated with the warranty (including

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

the purchase by the individual of an extended warranty), and be so be specified in execution of the organization's ILCM.

The sale of many types of goods or services require the seller to inform the buyer 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.

Rule 058:

Where the buyer in a business transaction is an individual, the seller shall inform the individual of (1) any and all records retention requirements of personal information which is recorded as the result of the actualization of the business transaction, including personal information which is required to actualize the business transaction, and (2) the time period(s) for which such sets of personal information are to be retained:

a) **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**

b) **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 business transaction.**

From a customer service perspective, many sellers, i.e. organizations (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, as well as obtaining client feedback, surveys, new product announcements, etc.

Rule 059:

Where the buyer in a business transaction is an individual, the seller shall inform that individual of the applicable SRI retention and associated ILCM conditions where these pertain to personal information.

It is important that when the buyer is an individual, prior to and at the actualization phase in a business transaction, the individual is fully informed by the seller of its records retention requirements and practices of the seller 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 business transaction, that certain types of personal information may be subject to differing records retention periods.

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

Rule 060:

Where a business transaction does not reach the actualization phase, any personal information collected by the organization in support of that transaction shall be deleted by the organization [unless the individual concerned explicitly provides his/her informed consent to the (prospective) seller with respect to the retention of such personal information, i.e., SPIs for a seller requested for a defined period of time].

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

It is noted that this rule makes provision for the possibility that the individual, as a prospective buyer, may consent to be kept informed by the seller about product information, e.g., via a catalogue, special

sales, new offerings, etc. Such a decision by the individual is of the nature of obtaining "informed consent".

Particular care needs to 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 Rule 028 in Clause 6 of a purchase and payment, it may not be necessary for the seller to know the actual personal identity of the buyer, but to have an identifier by which that buyer may be uniquely identified to the seller.

It may be sufficient that the seller is certain of payment because the seller 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 buyer and seller in order to fulfil its requirements in the transaction (but not the content of the transaction), whilst the seller does not need to know the identity of the buyer.

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 do not need to be able to identify the individuals within the public administration actually involved (although the internal functions of the public administration may need that information for their own supervisory purposes).

8 Rules governing the specification of ILCM aspects of personal information

8.1 Overview[23)]

The purpose of this clause is to bring forward, in an integrated manner and in an Open-edi context, applicable concepts and their definitions as well rules and related normative text found in ISO/IEC 15944-5 and ISO/IEC 15944-8, in the particular context of this document which focuses on privacy protection of personal information in the context of an ILCM nature requirements:

1) those pertaining to state changes in the sets of recorded information (at whatever level of granularity); and

2) those pertaining to records retention requirements, including assured disposition, i.e., expungement of personal information.

As such, the purpose of this clause is to bring forward normative text, rules and associated coded domains from ISO/IEC 15944-5:2008, 6.6.4.2 and 6.6.4.3 and present them in an amended form, as and where required, in the context of privacy protection requirements focusing on ILCM aspects. (This approach is similar to that taken for Clause 7 which also applies normative text from other parts of the ISO/IEC 15944 series and applies it in a privacy protection requirements and ILCM context.)

Generic aspects of external constraints of jurisdictional domains as rules and definitions governing business transactions are found in ISO/IEC 15944-5.

Users of this document are advised to familiarize themselves with the rules, definitions and associated text of ISO/IEC 15944-5:2008, 6.6.4.

Within a data management and interchange context, it is important that parties to a business 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 (SRIs) in their IT systems (as especially those in their DMAs). This includes both state changes as well as records retention and scheduling requirements. This pertains to basic information life cycle management (ILCM) principles in support of information law compliance (see Clause 5).

The need for information law compliance is mandatory when the set(s) of recorded information pertain to a business transaction, i.e., a "commitment exchange", where the buyer is an individual.

23) The tables, (coded domains) in Clause 8 are amended and a more detailed version of the original coded domains as found in ISO/IEC 15944-8.

These generic Open-edi aspects and rules pertaining to a business transaction are mandatory in any business transaction context which involves an individual as a buyer. This is because, where this is the case, privacy protection requirements apply. The generic aspects of external constraints of jurisdictional domains of a privacy protection nature as rules and definitions governing business transactions are found in ISO/IEC 15944-8.

A common requirement of external constraints of a public policy nature is that they mandate records retention (and deletion) requirements (consumer protection, privacy protection, etc.). In order to bridge legal, operational, public policy and IT perspectives, records retention is defined as in an Open-edi context[24] as:

> ***Open-edi records retention and disposal schedule (Oe-RRDS)***
> *specification of a period of time that a* ***set of recorded information (SRI)*** *shall be retained 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* ***business transaction***

As stated in ISO/IEC 15944-1, records retention requirements need to be specified:

— in the scoping of an Open-edi scenario (e.g., as a post-actualization requirement of a data component requirement);

— as an attribute of an information bundle (e.g., for specifying internal constraints) (see ISO/IEC 15944-1:—, 8.5.2.8 and Rule 140; and for external constraints see ISO/IEC 15944-1:—, 8.5.2.9 and Rule 141).

It is important to be able to specify which of the parties to a business transaction is responsible for retention of IBs or the complete set(s) of recorded information.[25] Many, if not most, of the privacy protection requirements are of an information management nature. A key reason here is that privacy protection requirements are a type of information law. Consequently, the integrated set of information life cycle management (ILCM) principles applies.

Rule 061:

Management and control of state change, retention and destruction of personal information shall be based on the application of the integrated set of information life cycle management (ILCM) principles.

It is noted that where an SRI life cycle pertains to or contains an SPI(s), that in such cases privacy protection requirements of an ILCM nature apply, i.e., are mandatory.

8.2 Rules governing establishing ILCM responsibilities for personal information (PI)

It is important in the modelling of a scenario for a business transaction that one establishes which party (or combination of parties) to the business transaction has (primary) responsibility for ILCM aspects.

Rule 062:

Where an individual is a buyer to a business transaction, the seller shall specify who is responsible for the retention and disposal of any (combination) of SRIs and in particular all SPIs

---

24) 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-business, e-government, etc. (an Open-edi context), a unique label or term has been invented: Open-edi records retention and disposal schedule (Oe-RRDS). This definition links to privacy protection requirements in that these are legal or regulatory in nature.

25) The concept of "information bundle (IB)" pertains to the grouping of one or more semantic components (SCs) of data interchanged among Open-edi parties to a business transaction. From a data management perspective, and in an ILCM context, the concept of "set of recorded information (SRI)" is used. A SRI can be the content value of a single data element, several grouped and managed together, a complete record or file, etc.

and do so during, or before, the negotiation phase and no later than at the actualization phase in accordance with privacy protection requirements.

Guideline 062G1:

Unless requested or negotiated otherwise, the default is that the Person in the role of seller is responsible for all aspects of ILCM of the SRIs pertaining to a business transaction and especially all SPIs.

Rule 063:

Where an individual is a buyer in a business transaction, the seller shall ensure that all other parties to the instantiated business transaction, as applicable (e.g., a regulator, an agent and/or third party), are informed of records retention (and disposal requirements) and agree to abide by and support them.

Guideline 063G:

In support of Rules 062 and 063, the seller, as well as any other parties to the business transaction involving an individual as buyer (e.g., a regulator, an agent, and/or third party), should use coded domain 01 codes representing specification of ILCM responsibility for personal information (PI) where the buyer is an individual. This coded domain is presented in Table 1.

Guideline 063G2:

The nature of the goods, services, and/or rights of the business transaction may limit or specify which of the options in coded domain 01 can be used or are valid.

Guideline 063G3

Use of an ID code 02 in coded domain 01 is considered a "rarity" and the individual as a prospective buyer in a business transaction should be informed of the rationale for being responsible for ILCM requirements pertaining to the relevant personal information.

Rule 064:

Unless otherwise specified by the seller, the business transaction identifier (BTI) shall serve as its common unique ID for the instantiated business transaction for linking ILCM requirement to applicable SRIs.

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 business transaction where the individual is the buyer and (2) the assured destruction of personal information based on both legal requirements and contractual obligations (see Annex D).

Table 1 — 01: Codes representing specification of records retention responsibility for personal information (PI)

01: Codes representing specification of ILCM responsibility for personal information (PI) where the buyer is an individual				
IT interface			Human interface equivalents (HIEs): linguistic — written form	
Source authority ID	Coded domain ID	ID code	ISO English	ISO French
15944-12	01	00	Other If Code "00" (Other) is used, there should be an associated linked data element to capture the data value of the "Other".	autre
15944-12	01	01	Seller is responsible for all ILCM aspects and shall inform the buyer of what they are.	
15944-12	01	02	Individual as buyer is responsible for ILCM aspects and the seller shall specify what these are.[a] The seller shall inform the buyer of the basis as to why ILCM responsibilities are assigned to the buyer.	
15944-12	01	03	Seller and buyer are both responsible and seller shall inform the buyer, as an individual, what his/her ILCM responsibilities are.	
15944-12	01	04	Seller shall specify to the individual as buyer what specific IBs to retain resulting from the business transaction.	
15944-12	01	05	Seller and individual shall use a common third party, (e.g., a notary).	
15944-12	01	06	Regulator is responsible for retaining the personal information.[b]	
15944-12	01	07	Regulator and seller are responsible.	
15944-12	01	08	Regulator and individual are responsible. (The buyer as individual is informed of the personal information being retained.)	
15944-12	01	09	Regulator, buyer and individual are all responsible. (The buyer as individual is informed of the personal information being retained.)	
15944-12	01	10	Regulator mandates the involvement of a (role) qualified or designated third party, i.e., on behalf of seller, the individual and regulator.[c]	
15944-12	01	98	not known	inconnu
15944-12	01	99	not applicable	sans objet

[a] Use of ID code 02 is a "logical" possibility. Its use is considered a "rarity".

[b] An example would be the personal information for a driver's licence, or any other transaction where the regulator is the "authoritative" source.

[c] Examples include notarial acts, a regulator assigning a record-keeping registry, etc., function to a third party.

8.3 Rules governing establishing specifications for retention of personal information (PI) — applicable "SRI retention triggers"

External constraints of a record retention nature have requirements which specify (1) when a retention requirement is to start, i.e., via a limited number of triggers and (2) a specified (minimum) retention period. On the whole, records retention requirements are triggered by an action or event. The basic conditions from an external constraints perspective for "retention triggers" are limited. The most common ones are presented in coded domain 04 of ISO/IEC 15944-5 (see ISO/IEC 15944-5:2008, Annex F). It has been amended in the context and focus of this document.

Rule 065:

Where an individual is a (potential) buyer to a business transaction, the seller shall specify the "retention triggers" activating records retention requirements for the SRIs (and any combination of the same) pertaining to that business transaction and do so in accordance with applicable privacy protection requirements of the applicable jurisdictional domain(s) for that business transaction.

Guideline 065G1:

The seller, as well as any other parties to the business transaction (e.g., a regulator, an agent, and/or third party), should use coded domain.

Table 2 — 02: Codes representing SRI retention triggers for retention of personal information (PI)

02: Codes representing SRI retention triggers for retention and disposition of personal information (PI)				
IT interface			Human interface equivalents (HIEs): linguistic — written form	
Source authority ID	Coded domain ID	ID Code	ISO English	ISO French
15944-12	02	00	Other If Code "00" (Other) is used there should be an associated linked data element to capture the data value of the "Other".	autre
15944-12	02	01	Start applicable required retention period at the date/time for set(s) of recorded information as received, created and/or collected as part of the "identification phase" of the business transaction.	
15944-12	02	02	Start applicable required retention period at date/time for set(s) of recorded information as received, created or collected as part of the "actualization phase" of the business transaction (including those based results of completion of the "negotiation phase").	
15944-12	02	03	Start applicable required retention period from date of last action or use of the SRIs with respect to the business transaction.	
15944-12	02	04	Start applicable required retention period at end of calendar year when the business transaction was completed at end of the "actualization phase".	
15944-12	02	05	Start applicable required retention period at end of fiscal year when the business transaction was completed at end of the "actualization phase".	
15944-12	02	06	Start applicable required retention period at end of calendar year when the business transaction was completed at end of the "post-actualization phase".	
15944-12	02	07	Start applicable required retention period at end of fiscal year when the business transaction was completed at end of "post-actualization phase".	
15944-12	02	99	not applicable[a]	sans objet

[a] This would apply to recorded information, i.e., a particular SRI, deemed to be ephemeral or transitory in nature (such as a "session cookie").

It is also important to state the actual retention period, i.e., temporally. At the same time, it is a not uncommon occurrence that privacy legislation, or pursuant regulation, does contain a minimum temporal period for the retention of personal information, particularly where such personal information pertains to decision-taking or commitment-making such as takes place in the formation of a business transaction.

In many jurisdictional domains (e.g., consumer protection-based) it is a requirement that the potential buyer is fully informed of all the conditions which apply to an eventual purchase of a good, service and/or right. Similarly, privacy protection requirements require informed consent with respect to any collection, use, sharing, retention, etc., of personal information where the buyer is an individual. This includes the seller providing full and complete information on the duration of the retention of personal information. These and related requirements are captured in the following rules.

The record retention period(s) for SRIs and associated IBs (and SCs) need to be specified and stated explicitly. The retention period is independent of the retention triggers.

Rule 066:

The period that recorded information pertain to a business transaction, where the individual is a buyer, is retained (as once or more SRIs) shall be specified and made known to the individual.

Guideline 061G1:

In support of Rule 066, the seller as well as any other party(ies) to the business transaction (e.g., a regulator, an agent and/or third party), should use coded domain 03.

Rule 067:

Where the (prospective) buyer is an individual, the seller shall inform the buyer of minimum record retention period(s) of applicable privacy protection requirements which apply where a business transaction enters the "identification phase" and further.

Guideline 067G1

Sellers should apply Rule 050 as a best business practice and inform all buyers of the applicable minimum retention period for SRIs of buyer information.

Rule 068:

Where the (prospective) buyer is an individual, the seller shall inform the buyer of a maximum record retention period(s) of applicable privacy protection requirements which apply where a business transaction enters the "identification phase" and further.

Guideline 068G1

Sellers should apply Rule 068 as best business practice and inform all buyers of their applicable maximum retention period for SRIs of buyer information.

Rule 069:

Where the (prospective) buyer is an individual, the seller shall inform the buyer of any record retention period(s) as required by applicable laws or regulations requirements which apply and which "override" those of a privacy protection nature, including "permanent" retention where a business transaction enters the "identification phase" and further.

Rule 070:

Where the (prospective) buyer is an individual, the seller shall inform the buyer of the record retention period(s) of applicable privacy protection requirements (other than those of a minimum or maximum nature) which apply where a business transaction enters the "identification phase" and further.

Table 3 — 03: Codes representing the specification of types of record retention period

03: Codes representing the specification of types of record retention period				
IT interface			Human interface equivalents (HIEs): linguistic — written form	
Source authority ID	Coded domain ID	ID code	ISO English	ISO French
15944-12	03	00	Other If Code "00" (Other) is used, there should be an associated linked data element to capture the data value of the "Other".	autre
15944-12	03	01	Minimum retention period is stated in applicable privacy protection requirements.[a]	
15944-12	03	02	Maximum retention period as stated in applicable privacy protection requirements. (Seller to provide information to individual as buyer.)[b]	
15944-12	03	03	Nature of the good, service and/or right as the goal of the business transaction invoke other minimum retention periods which of a longer temporal nature than that of privacy protection requirements.[c] (Seller to provide information to individual as buyer.)	
15944-12	03	04	Nature of the good, service and/or right as the goal of the business transaction requires permanent retention of specified personal information.[d]	
15944-12	03	05	The retention period is specified using date/time referencing based on the ISO 8601 series, i.e. a temporal period specified in years, months, weeks, days, hours, minutes, etc. (the Gregorian calendar).[e]	
15944-12	03	06	The retention period is specified based on a temporal referencing schema other than that based on the ISO 8601 series, and, if so, this needs to be specified.[f]	

[a] A common default for personal information is two (2) years after business transaction completed. For SRIs of a financial nature, it is a minimum retention period of seven (7) years. At times, it is possible that telecom and internet service providers are required to maintain personal information on their users for a minimum period of time (six months, two years, etc.).

[b] For example, IBs pertaining to the use of a telecom service often have a maximum retention period after which the telecom deletes the record of the same. This varies per jurisdictional domain.

[c] An example would be financial information pertaining to an actualized business transaction where financial information possibly has to be retained for a minimum of seven years.

[d] A code "04" would apply to the purchase and sale of what are commonly known as "immovables" (a piece of land, a house, etc.)

[e] On temporal referencing, see ISO/IEC 15944-5, 6.6.4.5.

[f] See footnote 22. ISO/IEC 15944-5 provides information on other temporal referencing schemas such at the "atomic clock", the "GPS calendar/clock", etc.

8.4 Rules governing identification and specification of state changes of personal information (PI)

8.4.1 General requirements

This clause integrates text and rules from ISO/IEC 15944-5:2008, 6.6.4.3 and ISO/IEC 15944-8:2012, F.2.

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 (SRI). 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 ISO/IEC 15944-1:—, 5.4). As such, it is important to know whether or not the value of an information bundle (IB) (or one of its semantic components (SCs) interchanged among parties to a business transaction is allowed to be changed during any stage in the process component. Knowing whether or not state changes are allowed for a specific IB or SC is important for the management of state description and automated change management of the state machines of the parties involved in an electronic business transaction.

This is a requirement which also exists in modelling business transactions involving internal constraints only. However, those which exist here are likely to be a sub-set of those which arise from external constraints.

During the life cycle of a business transaction (i.e., from its planning through post-actualization phases), there are more SRIs of a personal information nature that pertain to the business transaction which may require a state change to their content value(s). For example, the address of the buyer as an individual may change; the planned delivery date or delivery location may change, etc.

At the same time, there are SRIs pertaining to personal information in a business transaction for which no state changes are allowed, e.g., the business transaction identifier (BTI).

It is also understood that, with respect to any personal information pertaining to an individual as a party to a business transaction, privacy protection requirements apply.

Rule 071:

Where the recorded information pertaining to a business transaction contains personal information (as one or more SRIs), the seller shall specify: (a) for which SRIs, there will be no state changes; and (b) for which SRIs state changes are allowed and, if so, under which conditions.

Rule 072:

In a business transaction involving an individual as buyer, the seller shall inform and obtain informed consent from the buyer, as individual, to any state changes to any SRIs pertaining to the business transaction, including those forming the basis for one or more SCs or SRIs, as IBs in EDI with parties to a business transaction.

A related issue is “What happens to recorded information, i.e., SRIs, which existed prior to a state change being made?” It is important for parties to a business transaction to know this. To address this issue, two attributes are required to specify state change of data. They are:

— number of state changes allowed, if any; and

— 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 each IB and SC. It also covers which actions are required with respect to both “new” and “old” data including those required for information life cycle management (ILCM) within an organization, audit trails, evidentiary requirements, disposition/ expungement, etc., and any external constraints of this nature of jurisdictional domains.

8.4.2 Specification of state changes allowed to personal information (PI)

Before any information is recorded at any phase in a business transaction it is important to establish whether or not such recorded information may be changed, i.e., undergo a "state change" of the initial value(s) recorded. Examples of an SRI whose value is recorded with respect to the instantiation of a business transaction, for which a state change is not allowed, is the business transaction identifier (BTI). Others include those SRIs which, when shared via EDI as SCs and IBs with parties to a business transaction, are not allowed to undergo a state change due to applicable external constraints.

Rule 073:

Where an individual is a party to a business transaction, i.e., as a buyer, the seller (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 ILCM and EDI required to comply with privacy protection requirements.

Rule 074:

Where the buyer is an individual, the seller shall inform the buyer whether or not state changes will be allowed for one or more of the SRIs constituting the recorded information pertaining to that business transaction.

Guideline 074G1:

Depending on the nature of the good, service and/or right which is the goal of the business transaction, external constraints of applicable jurisdictional domain(s) may prohibit a state change to one or more SRIs.

An example of an IB (or SC) having a Code "09" with respect to state changes would be in item tracking in a logistics system (e.g., the seller provides to a buyer a facility to access the seller's or logistic provider's system to track the movement of an item to be delivered to the buyer). The content value of the related SRI would undergo state changes of a dynamic basis.

Guideline 074G2:

If several SRIs pertaining to a business transaction are allowed to be changed, care is required to be taken to prevent the business transaction from transforming itself into a completely new business transaction. A factor to be considered is for those SRIs allowing (too many) changes, which may lead to "disharmony" among the various SRIs, thereby compromising the integrity of the recorded information on a business transaction.

Rule 075:

An instantiated business transaction shall have one or more IBs or SCs for which no state changes are permitted. One of these is to serve as the transaction ID number, i.e., a business transaction identifier (BTI), for the instantiated business transaction.

Guideline 075G1:

It is advised that in modelling scenarios, scenario attributes roles, information bundles and scenario components, the state change code is set to "00" wherever applicable, especially for those pertaining to personal information.

This guideline serves to ensure that all parties to a business transaction agree to, and have knowledge of, permitted state change to the value of an IB or SC.

Rule 076:

If a state change is required, the seller (and/or regulator) shall specify the number of state changes permitted.

Guideline 076G1:

In support of Rules 075 and 076, the seller, as well as other parties to the business transaction as applicable (e.g., the regulator, an agent, or third party), should use coded domain 04 to specify the applicable state change ID codes.

Table 4 — 04: Codes for specifying whether state changes allowed for the content values of SRIs containing personal information (PI)

04: Codes for specifying whether state changes allowed for the content values of SRIs containing personal information (PI)				
IT interface			Human interface equivalents (HIEs): linguistic — written form	
Source authority ID	Coded domain ID	ID code	ISO English	ISO French
15944-12	04	000	**no state change allowed (default)**	
15944-12	04	010	One state change allowed as per nature of business transaction.	
15944-12	04	011	One state change allowed as requested by buyer as an individual.	
15944-12	04	012	One state change allowed as requested by the seller and consented to by the buyer as an individual.	
15944-12	04	013	One state change allowed as may be required by the regulator.	
15944-12	04	020	Two state changes allowed as per nature of business transaction.	
15944-12	04	021	Two state changes allowed as requested by buyer as an individual.	
15944-12	04	022	Two state changes allowed as requested by the seller and consented to by the buyer as an individual.	
15944-12	04	023	Two state changes allowed as may be required by the regulator.	
15944-12	04	030	Three state changes allowed as per nature of business transaction.	
15944-12	04	031	Three state changes allowed as requested by buyer as an individual.	
15944-12	04	032	Three state changes allowed as requested by the seller and consented to by the buyer as an individual.	
15944-12	04	033	Three state changes allowed as may be required by the regulator.	
15944-12	04	090	No limit on the state changes allowed as per nature of the business transaction.	
15944-12	04	091	No limit on the state changes allowed as requested by the buyer as individual and agreed to by the buyer as an individual.	
15944-12	04	092	No limit on the state changes allowed as per nature of the business transaction as requested by the seller and agreed to by the buyer as an individual.	
15944-12	04	093	No limit on state changes allowed as may be required by the regulator.	

An example of use of code "000" would be the transaction record ID number as the business transaction identifier (BTI) (see ISO/IEC 15944-8:2012, 11.2) i.e., the unique ID number assigned by the seller to an instantiated business transaction. Codes "1", "2", "3", etc., are used to deal with IBs and SCs pertaining to location information, such as physical or electronic addresses, price and terms negotiations, the buyer changing its decision on a choice of options, etc.

8.4.3 Specification of store change type

It is important to specify clearly and explicitly the action to be taken and the processes to be followed by the seller (as well as its agents and third parties) with respect to the original content value of an

SRI (and related IBs and SCs) when the content value for these is changed during any of the phases in a business transaction. The key issues addressed in the following rules and Table 5 are "What happens to the original data value(s) entered when a state change for it is permitted to occur? Is the original data value simply deleted or does it need to be retained?"

Rule 077:

If a state change is permitted to the original data value of the SRI and resulting IB (or its associated SCs), i.e., (1) any entered in the DMA(s) of the IT system(s) of the organization or public administration which acting in the role of a seller or a regulator in a business transaction involving an individual and/or (2) as interchanged among the Persons involved, it is necessary to specify in the business object being modelled the store change type permitted.

Guideline 077G1:

The seller, as well as other parties to the business transaction as applicable (e.g., the regulator, an agent or a third party) should use coded domain 05 to specify store change type.

The ID code in this coded domain defines and specifies what action is to be taken when a state change in the content value of an SRI is allowed. This is necessary to support required audit trails, data integrity and ILCM including archiving/disposition requirements as well as from a legal/evidentiary requirements perspective. The ID codes for store change type in Table 5 identify whether the previous content value of an SRI is required to be retained, in addition to the most current data value. If it is not required, the new value can replace the existing content value. If an audit history is required to be maintained then the relevant DMA in the IT system of the seller (and its agents and/or third parties) is required to be able to maintain multiple versions of the content value of the SRI including possible associated IT systems-generated date/time stamps.

EXAMPLE By analogy, an historical record of changes to the balance in one's bank account. Another example, (linked to ISO/IEC 15944-9) is that of traceability data in the form of SRIs pertaining to the movement/logistics of a "good" being delivered from a seller to a buyer.

Table 5 — 05: Codes representing store change type for SPIs (and SRIs)

05: Codes representing store change type for SRIs as information bundles and semantic components				
IT interface			Human interface equivalents (HIEs): linguistic — written form	
Source authority	Coded domain ID	ID code	ISO English	ISO French
15944-12	05	00	Other If Code "00" (Other) is used there should be an associated linked data element to capture the data value of the "Other".	autre
15944-12	05	01	Store new data value for the specified SRI and expunge previous data value.	
15944-12	05	02	Store new data value, expunge previous value for the specified SRI with date/time stamp when state change occurred.	
15944-12	05	11	Store new data value for the specified SRI and previous data value only.	
15944-12	05	12	Store new data value for the specified SRI and previous data value for the specified SRI only and add a date/time stamp.	

[a] For example, a code 99 here is automatic when a code 00 was assigned to the SRI or SPI based on coded domain 4 in ISO/IEC 15944-12.

Table 5 *(continued)*

05: Codes representing store change type for SRIs as information bundles and semantic components				
IT interface			**Human interface equivalents (HIEs): linguistic — written form**	
Source authority	**Coded domain ID**	**ID code**	**ISO English**	**ISO French**
15944-12	05	21	Store new data value for the specified SRI and "nn" previous values for the specified SRI maintaining a sequence number of all state changes. here "nn" is required to be specified.	
15944-12	05	22	Store new data value and "nn" previous values maintaining security and maintaining a date/time stamp for each state change. Here "nn" is required to be specified set of unique identifiers.	
15944-12	05	31	Store new data value for the specified SRI and all changes maintaining a sequence number of all state changes for the specified SRI.	
15944-12	05	32	Store new data value for the specified SRI and all changes, maintaining a date/time stamp for each state change for the specified SRI.	
15944-12	05	99	**not applicable, i.e., no state change allowed**[a]	

[a] For example, a code 99 here is automatic when a code 00 was assigned to the SRI or SPI based on coded domain 4 in ISO/IEC 15944-12.

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 business transaction.

8.4.4 Rules governing specification of source of state changes

There are three primary sources of state changes to SRIs pertaining to a business transaction: (1) those initiated by the buyer; (2) those initiated by the seller; and (3) those required by applicable external constraints.

The state change requirements of these three sources are not necessarily exclusive and may well be complementary to each other.

Rule 078:

In order to comply with privacy protection requirements, the source of the state change to a content value of any SRI forming part of a business transaction shall be specified as seller, buyer and/or an external constraint.

Guideline 078G1:

The seller, as well as other parties to the business transaction as applicable (e.g., the regulator, an agent or a third party), should use coded domain 06 to specify the source of state change type (and an ID code of "99" for those SRIs for which no state change is allowed). It is noted that use of one or more of the ID codes in this coded domain are not exclusive but may well be complimentary.

Rule 079:

Where the state change code in Table 4 is "000", i.e., no state change allowed, then code "99" in Table 5 (not applicable) applies and shall be used.

Table 6 — 06: Codes representing source of state change type ID code for SRIs

06: Codes representing source of state change type ID code				
IT Interface			Human interface equivalents (HIEs): linguistic — written form	
Source authority	Coded domain ID	ID code	ISO English	ISO French
15944-12	06	01	Buyer originated, i.e., the buyer as an individual is the only one who can request a state change to the content of one or more SRIs pertaining to a business transaction.	autre
15944-12	06	02	Seller originated, i.e., those which the seller identifies and proposes to the buyer as state changes associated with the business transaction.	
15944-12	06	03	Regulator originated, i.e. those which apply to the nature of the good, service and/or right and which are identified as such by the seller to a (prospective) buyer in a (proposed) business transaction.	
15944-12	06	11	The seller has informed the buyer of conditions pertaining to ID codes 01, 02 and 03; and, the buyer has agreed to the application of a combination of the same, i.e., as a result of the negotiation phase, with respect to the business transaction to be actualized.	
15944-12	06	99	Not applicable, i.e., no state change is allowed, (therefore source of state change does not apply).	

8.5 Rules governing disposition of personal information (PI)

This clause integrates text and rules from ISO/IEC 15944-5:2008, 6.5.4.3 and ISO/IEC 15944-8:2012, F.4. It does so in a privacy protection requirements context and from a more granular, ILCM-needs perspective.

A key privacy protection requirement is that of the mandatory destruction of personal information, i.e. as the reverse of records retention. Within an information/records management and archiving context, this process requirement of an organization 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[26]. In the context of this document, "Open-edi disposition" is defined in 3.77.

In this document, only the more basic, i.e., primitive, disposal actions are identified. However, even this limited set covers more than 85 % of the statutory requirements and best business practices of most organizations worldwide, and especially those of public administrations.

A key aspect of a "disposition" action is that the specified SRI(s) is removed from the normal and ordinary course of business use of the organization, i.e. "control". Another key aspect of any disposal action is that no state changes of any kind are allowed to the content value of any SRI(s) which has been "disposed" by the organization.

While the normal default result of a disposition action is the destruction (i.e., expungement) of the recorded information, it is not uncommon for other results of a disposition action to occur. Examples of these include:

— The transfer of the "disposed" SRI(s) to an archive (IT system) within the organization, and if so with the same or different access and use controls.

26) 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).

EXAMPLE 1 When an SRI(s) has as disposal action to be assigned the status of "archival", it is normally physically removed from the DMA of the organization and transferred to the "archival IT system" of the organization at which time access to and use of such SRI(s) fall under the control of the "archivist" as an officer of the organization.

— The transfer of the "disposed" SRI(s) to an archive (IT system) of (a) an agent of the organization; (b) an organization which is a third party to the organization; or (c) a totally separate, and largely removed, separate organization.

EXAMPLE 2 For (a): an organizational entity of a public administration, i.e. an organizational entity of a jurisdictional domain government organization which has established a separate and distinct organizational part" as a separate entity governed by separate legislation, regulation (or similar legal instrument). As a result, it is possible that such an organizational entity has its own distinct legal basis and associated rules for access to and use of such associated personal information for all the SRIs which constituting the specified "archival collection" for that natural person which are physically (and logically) maintained as a distinct "collection" the specified archival repository.

In addition, it is not an uncommon occurrence for all the personal information (public or private) for a "very important person" (VIP) in an organization to be transferred to a new separate organization, or legal entity within an existing organization, e.g., as a presidential archive, a prime ministerial archive or a private archive (including those of a university).

EXAMPLE 3 For (b): A private sector organization disposing of its specified SRIs to a university or a private sector (often non-profit) organization.

— The transfer of personal information by an organization for (officially recognized) research purposes; along with associated legally-supported access and use requirements, including formally accepted (and legally permitted) access and use protocols. These are normally specified via formal rules (and associated guidelines) and supported by applicable coded domains as necessary/applicable. Here such transfers may need to incorporate or ensure "individual anonymity", i.e., all PIs being anonymized.

EXAMPLE 4 Public administrations providing personal information on specified data elements relating to an (identified) individual on a systematic (including continuous) basis with respect to an officially approved research project.

Rule 080:

Where the buyer in a (prospective) business transaction identifies himself/herself as an "individual" in the "identification phase' of a business transaction, the (prospective) seller shall inform the (prospective) buyer of any and all ILCM conditions and options as part of the applicable personal information privacy protection requirements and associated rules required to be provided by the buyer as part of the "planning phase' or, at the latest, at the end of the "identification phase" of a potential business transaction.

Rule 081:

Where an individual is a buyer to a business transaction, the seller 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 as well as those applicable to the nature of the product, service and/or right which is the agreed upon goal of the (to be) actualized business transaction, and in particular those SRI retention requirements which are mandatory based on the nature of a the good, service and/or right which is the agreed upon goal of the business transaction.

Guideline 081G1:

The seller, as well as any other parties to the business transaction (e.g., a regulator, an agent, and/or third party), should use coded domain 05.

It is also a common and well-established practice for sets of personal information (SPIs) to be scheduled and disposed of by transfer to an archive for historical and research purposes. As a matter of fact, many jurisdictional domains have in place legislation (and pursuant regulations) for this purpose (e.g., in the

form of a “national archives act”, a “medical research act", legally enforced protocols governing access and use of personal information retained as part of longitudinal research, sampling). This is especially so with respect to public administrations.

On the whole, once an SPI is “disposed”, according to the applicable RRDS, the content value(s) cannot be changes, i.e., if state changes were permitted on the SPI while it was active and being retained, once it is disposed no more state changes are allowed. Where SPIs, including SRIs, are not destroyed/expunged as the disposal action, they are transferred to an archive either within the organization itself or to archive of another organization as per (legal/contractual) agreement as supported by applicable information law.

Certain types of SRI and associated SPIs resulting from completing the goal of a business transaction may be required to be retained permanently. This is the case for various types of business transactions which do not have any “post-actualization” requirements. Examples of these include educational records, i.e. those pertaining to completion of high school, a degree at a college or university, sale and transfer of an immovable property, etc.

Rule 082:

Where the disposition action of an SRI, and in particular that of a SPI, is that of transfer to an archive to be retained permanently (i.e., as “permanent” SPI or SRI), no further state changes are allowed for the same.

Guidelines 082G1:

Where the condition of Rule 061 applies, it is recommended to use ID codes 11 or 12 in coded domain 07.

In addition, it can happen that the individual would like an organization to retain its SPIs (and associated SRIs) after the scheduled disposition date/action. This approach is provided for in privacy protection, where the organization is able to ask an individual whether or not PI collected for one purpose may be used and retained for another purpose.

EXAMPLE An organization establishes a dossier on an individual (with the individual’s consent) with respect to security clearance, level of competency, qualifications and so on, especially those which include letters of reference, certified copies of key documents, etc. It is possible that, according to applicable PPR, the particular applicable SPI(s) is mandated to be destroyed/expunged two years after last use. However, the individual concerned, having used significant resources and time to compile the dossier and have it accepted by the organization, could very possibly request that the organization retain such SPIs.

It may well be that, according to the applicable privacy protection requirements for the relevant SPI(s), these SPI(s) are mandated to be destroyed/expunged after two years of last use. However, the individual to whom these SPI(s) pertain may well wish to have those SPI(s) returned to that individual (whether as original or copies, electronic/digital form, etc.). One reason here is that an individual may have used significant resources and time to provide its personal information to the organization. Also, an individual has the right to request a copy of its SPI(s) from the organization at any time. Finally, where the SPI(s) are returned to the individual, one should consider using code 20 in Table 7.

Rule 083:

Where the disposition action of an SRI, and in particular that of an SPI, is that to be retained permanently for historical or research purposes (i.e., as a “permanent” SPI or SRI), no further state changes are allowed and the SPIs (or SRIs) are not subject to access and use conditions and no longer permitted to be used for decision-making actions with respect to the individual whose SPI(s) it is.

Guideline 083G1:

Where the condition of Rule 083 applies, it is recommended to use ID code 13 in coded domain 07.

Table 7 — 07: Codes representing disposition types as actions of personal information (as SPIs)

07: Codes representing disposition of personal information (as SPIs)				
IT interface			Human interface equivalents (HIEs): linguistic — written form	
Source authority ID	Coded domain ID	ID code	ISO English	ISO French
15944-12	07	00	Other. If Code "00" (Other) is used there should be an associated linked data element to capture the data value of the "Other".	autre
15944-12	07	01	Disposition as complete destruction, i.e., expungement, of the applicable SRI(s) by the organization which controls the ILCM aspects of the specified personal information as SPIs. This not only includes expungement by the seller as the originating institution, i.e. Person, but also ensuring that any of its associated agents and/or third parties, to the relevant business transaction.	
15944-12	07	02	Disposition as complete destruction, i.e. expungement, of the applicable SPI (and related SRIs) and notification to the individual of the disposal action.	
15944-12	07	10	Disposition via transfer to an archival institution for permanent retention or specified time period retention – General (no further state changes are permitted).	
15944-12	07	11	Disposition via transfer to an archival institution, for permanent retention, which functions as a separate legal entity. (When such a transfer takes place, no further state changes are allowed to the SPI(s) and its related SRI(s).)	
15944-12	07	12	Disposition via transfer to another organizational entity within the same organization, as an archival record, for permanent retention. (When such a transfer takes place, no further state changes are allowed to the SPI(s) and its related SRI(s).)	
15944-12	05	13	Transfer to an archival institution (for historical and research purposes). (When such a transfer takes place, no further state changes are allowed to the SPI(s) and its related SRI(s) and specified (new) access and use conditions apply.)	
15944-12	05	20	Destruction of the complete SRI, including its SPIs, by the organization with or without the return to the individual whose personal information it is (via a printout of the (final) record, an email with a pdf file, etc.)	
15944-12	05	80–89	User/implementing organization specified.	
15944-12	05	98	not known	inconnu
15944-12	05	99	not applicable[a]	sans objet

[a] This would apply to recorded information deemed to be transitory or ephemeral which can be discarded anytime, if the organization is able to ensure that such recorded information is not subject to any external constraints of an "information law" nature.

8.6 Rules governing the establishment and maintenance of record retention and disposal schedules (RRDS) for sets of personal information (SPIs)

Increasingly, the resources of an organization (and especially a public administration) are of the nature of "recorded information". This is also true of any organization in which EDI plays a significant role in the provisioning and delivery of goods, services and/or rights, especially those of an eBusiness nature.

In many organizations, apart from its human resources, sets of recorded information (SRIs) are its major resources.

A vital factor in efficient and cost-effective management of one's information resources is that of a systematic approach to 1) ensuring that the recorded information that one has is up-to-date, timely and relevant; and, 2) deciding what to keep, for how long, what to discard, etc. based on applicable internal and external constraints which, with respect to this document, require compliance with external constraints of a privacy protection requirements nature. Such a systematic approach is commonly known as the establishment of a "records retention and disposal schedule" (RRDS)[27].

The establishment of an RRDS is a key element in any ILCM-based approach. Basically, an RRDS prescribes the requirements of: 1) the length of time an SRI shall be retained while it is active part of the operation of the organization; 2) the criteria and appropriate disposal action of an SRI at the end of its life cycle. The primary sources of RRDS requirements are:

a) Internal constraints as established by an organization (and formally approved by its senior management) with respect to its ILCM approach to and policy for with respect to managing its resources in the form of recorded information – based on the nature of the good, services and/or rights that it provides.

2) External constraints, especially those of an applicable legal and regulatory nature, based on the nature of the goods, services, and/or rights which the organization provides to its clients. Where the client is an individual, the privacy protection requirements apply to any and all recorded information which is personal information (PI), i.e., SPIs.

Rule 084:

An organization shall ensure that it develops, adopts and implements a formally approved records retention and disposal schedule (RRDS) as part of its ILCM approach to compliance with requirements (of either an internal constraints and applicable external constraints of an information law nature) applicable to the goods, services and/or rights the organization provide.

Rule 085:

When and wherever an organization has under its control recorded information which is of the nature of personal information (PI), it shall ensure that either 1) its existing RRDS supports applicable privacy protection requirements; or 2) that it develops an RRDS, as part of its ILCM policy, which (fully) supports applicable privacy protection requirements. i.e., as specified in Clause 8.

In the context of ILCM requirements and the systematic and IT-enabled approach presented in Clause 8, key elements of an RRDS include for any SRI (and also any SPI):

a) The rules governing specification of the SRI retention trigger (see 8.3 and Table 2).

b) The rules governing specification of types of retention periods (see 8.3 and Table 3). Here the use of codes 01 or 02 is of particular relevance from a privacy protection requirements perspective.

c) The rules governing specification of whether or not any state changes are permitted for a SRI containing personal information and the source of the requirement for state changes (including the individual itself), and if so the number of state changes (see 8.4.2 and Table 4).

d) The rules governing specification of store change type for IBs and SCs. This is of particular importance in a PPR context as all state changes pertaining to personal information form part of an SPI (see 8.4.3 and Table 5).

27) It is outside the scope of this document to prepare rules for planning, establishing and maintenance of an RDDS. Examples are available from professional organizations in the fields of archiving, records management, information management etc., such as: https://www.alberta.ca/assets/documents/IM-Developing-Schedules.pdf or https://archives.un.org/content/retention-schedules
Public administrations in most countries have similar detailed documents on RRDS. In addition, ISO 15489-1 is also useful.

e) The rules governing specification of source of change state type. This is also of particular importance from a PPR perspective, especially where the buyer, as an individual in a business transaction, is the one who requests a change state in its SPI pertaining to the business transaction (see 8.4.4 and Table 6).

f) The rules governing specification of disposition types of all or parts of an SPI(s) pertaining to a business transaction and/or forming part of a personal information profile (PIP).

Guideline 085G1:

An organization should implement the rules and coded domains (as decision tables) in a systematic approach in support of the organization, as a seller in a business transaction, to a buyer, as an individual, in an integrated and IT-enabled manner in order to be able to comply with PPR in a cost-effective and efficient manner.

9 Data conversion, data migration and data synchronization[28]

9.1 Purpose

It is necessary to differentiate between:

a) information life cycle management which focuses on the "data" or content values themselves, and is a BOV perspective; and

b) system life cycle management (i.e. of IT systems, software), which is (should be) independent of any "data" and is basically an FSV perspective, i.e., the BOV requirements inform/instruct what FSV shall be able to support.

This approach is supported by the fact that Open-edi BOV standards, such as the ISO/IEC 15944 series, take a neutral approach to IT systems (see 0.13). As such, data conversion, data migration and data synchronization pertaining to privacy protection and ILCM requirements are quite independent of software and IT systems life cycle aspects.

One characteristic of information and communication technologies (ICT) is that many of its components have a relatively short life cycle. Examples include system upgrades, new and different software, data storage devices, data processing approaches, communication devices and protocols, etc. As such, it is not an uncommon occurrence that, during the lifetime of a business transaction, especially where a business transaction covers several years (including post-actualization), the organization, in the role of seller, undertakes a data conversion of its recorded information. Similarly, during the life time of the recorded information pertaining to a business transaction, it may well happen that the organization undertakes an IT systems upgrade, migration to another IT system, etc., with one result being a "data migration". In either case, it is essential that all ILCM requirements are maintained and, in particular, those pertaining to personal information.

A differentiation is made between (1) data conversion, which deals with/focuses on changes to the "format" and "representation" of the content of an SRI; and, (2) data migration, which deals with/focuses on changes to the medium of recording, IT system (but not the application software).

It is also necessary to ensure "data synchronization" of personal information pertaining to a business transaction, not only within all the DMAs of the IT system of the seller but also where the seller has an agent(s) or the nature of a business transaction involves the participation of a third party(ies) among the DMAs of the seller and its agents and/or third parties.

28) The principles and rules presented in this Clause incorporate existing requirements and long-established best practices in the records management and archival community with respect to microfilming standards, evidentiary requirements, etc.

9.2 Rules governing data conversion of set(s) of personal information (SPI)

NOTE This approach is based on that of ISO 13008.

It is necessary to differentiate between changes in the use of ICT by an organization which are (a) of the nature which impact the format and/or representation of the content of the SRI(s), i.e., "data conversion" which applies at the "format or representation level; and (b) of the nature which involves "data migration" of the SRI(s) from one IT system, data storage medium, etc., to another without any change to the application software used to manage and/or represent the contents of the SRIs pertaining to a business transaction.

In this context and in support of this e-business, it is necessary to differentiate between the concepts and definitions of data conversion and data migration as per 3.31 and 3.33.

Rule 086:

Where an organization undertakes a data conversion of its SRIs pertaining to a business transaction and the SRIs contain personal information (i.e., as part of an SRI and/or as one of more SPIs), the organization shall ensure that applicable ILCM aspects in support of privacy protection requirements are fully maintained (and carried forward).

Rule 087:

Where an organization undertakes a data migration of its IT system(s) to another IT system and that IT system contains SRIs pertaining to a business transaction and the SRIs contain personal information, i.e., as either part of a SRI and/or as one of more SPIs, the organization shall ensure that applicable ILCM aspects in support of privacy protection requirements are fully maintained (and carried forward).

Rule 088:

Whenever an organization undertakes a data conversion or a data migration, it shall maintain the authenticity, integrity, reliability and usability of the SRI(s) as well as relevant ILCM requirements, and especially those of an external constraints nature, including privacy protection requirements where the SRIs are of the nature of personal information.

Rule 089:

Whenever an organization undertakes a data conversion or a data migration, it shall maintain an audit log/audit trail to provide proof and evidence that the processes involved maintain the authenticity, integrity and reliability of the contents of the SRIs and in particular those which are of the nature of personal information.

Rule 090:

Whenever an organization plans to undertake a data conversion or a data migration pertaining to SRIs which contain personal information, it shall inform its privacy protection officer (PPO) and request its PPO to review and assess whether such data conversion or data migration plans, processes, audit trails/logs, etc., comply with and support applicable privacy protection requirements.

9.3 Rules governing requirements for data synchronization of sets of personal information (SPI)

The need to ensure "data synchronization" for the information bundles (IBs) [and their semantic components (SC)] interchanged among Open-edi parties to a business transaction has always been assumed. It is a fundamental and logical conclusion of the application of the six fundamental characteristics of Open-edi, especially from a BOV perspective.

Data synchronization is the process of establishing consistency of the content value(s), semantic components (SCs) and any SRI from the source IT system to and among any and all other IT systems

involved in a business transaction, and vice-versa, through ensuring continuous harmonization of data over time, i.e., whenever a state change occurs. Within IT systems of an organization, data synchronization can involve a number of tools such as referential integrity, file synchronization, version control, synchronized distributed systems, mirror computing and back-ups., etc., as well as timestamp synchronization, where all state changes to the content value are marked with time stamps. Data synchronization needs to be well designed and managed in order to prevent "sprawl" of data, and to ensure that data integrity safeguards are in place, security management can be implemented, etc.

Not only is ensuring data synchronization among the IT systems of Open-edi parties participating in a business transaction very important from both a BOV- and FSV-requirements perspective but, where the buyer is an individual, privacy protection requirements make data synchronization mandatory.

Rule 091:

Where the buyer in a business transaction is an individual, the seller (possibly using more than one DMA (or IT system) to process the SPIs pertaining to the instantiation of the business transaction) shall ensure that complete data synchronization exists or is enacted among all such DMAs (and their IT system) including those of a back-up nature.

Rule 092:

Where Rule 090 applies and the seller uses an agent and/or a third party, the seller shall ensure that data synchronization exists, or is enacted, prior to any EDI of SPIs with such parties.

Guideline 092G1:

A seller should make data synchronization capabilities for SPIs, as stated in Rules 090 and 091, a pre-condition as part of a contractual agreement before engaging in EDI with any agent and/or third party with respect to SPIs pertaining to a business transaction.

Privacy protection requirements (PPR) allow for state changes to the content value of semantic components (SCs) forming part of a set of personal information (SPIs) in business transactions under certain and specified conditions. These and associated rules and guidelines are summarized in 8.4. This includes the seller ensuring that when a state change occurs in the DMA(s) in its IT system(s) pertaining to all or part of a set(s) personal information (SPIs) on a buyer as an individual in an instantiated business transaction, that the same state change occurs in the content value of SPI(s) maintained by all parties with which the seller, via EDI, has made parties to that business transaction as either agents or third parties. This requirement also applies to any and all coded domains pertaining to, and used as, references with respect to parties and their IT systems involved in a business transaction. This operational if known as "transactional integrity" and in a PPR context is labelled as "privacy protection transactional integrity" (PPTI), which is defined in 3.99.

Rule 093:

Where in a business transaction the buyer is an individual, the seller shall ensure that: 1) in its own IT system(s) it has in place policies and procedures which ensure that privacy protection transactional integrity (PPTI) requirements are supported; and 2) any, and all, of the agents and/or third parties which the seller involves, via EDI, in the execution of an instantiated business transaction also have in place policies and procedures which ensure that they are able to and will support PPTI requirements in their IT system(s).

Guideline 93G1:

Any organization (including public administrations) should ensure that, prior to involving any agents and/or third parties in the instantiation of a business transaction, these parties are capable of and do implement PPTI requirements.

To conclude, one should view PPTI requirements with respect to personal information as being similar in nature to existing requirements of a transactional integrity nature in "real time" (business) transactions in sectors such as finance and banking services, logistics and management services, medical services,

etc.[29] In these and other sectors that support PPTI requirements, it is vital that all parties to a business transaction, engaging in EDI ensure that the state of their recorded information pertaining to any business transaction including state changes, remains harmonized and is synchronized with respect to the content value of a data element at whatever level of granularity.

10 Rules governing EDI of personal information (PI) between primary ILCM Person, i.e., the seller, and its "agent", "third party" and/or "regulator"

10.1 General requirements

This clause integrates and summarizes existing rules from ISO/IEC 15944-1:—, 6.2.3 to 6.2.6 and of applicable clauses in ISO/IEC 15944-8 such as ISO/IEC 15944-8:2012, 5.3.2.

This clause focuses on EDI aspects of personal information, i.e., criteria and rules which are required to be complied with by both the primary ILCM Person (i.e., the seller) and a prospective "agent" and or "third party" prior to the seller deciding to use an "agent", or "third party" as a separate autonomous party, in support of an instantiated business transaction where the buyer is an individual.

The increased use of organizations to outsource some, or most of, their IT systems including their DMAs and related processing to "cloud-based" services increases the important of ensuring that applicable ILCM aspects of SPIs continue to be supported (see ISO/IEC 15944-8:2012, 5.3.2).

With respect to the engagement of a third party in a business transaction, it is already stated in ISO/IEC 15944-1:—, 6.2.5, that a third party is not an agent of either the buyer or seller but is one who fulfils a specific role or function in the execution of a business transaction as mutually agreed to by the two primary Persons or as a result of applicable external constraints.

One current approach to offering supporting ICT-based services to an organization (or public administration) as a seller in a business transaction is now known as cloud computing.

Rule 094:

The rules governing the delegation to an agent and/or third party by either the seller, buyer and/or regulator of any aspect of the commitment exchange(s) among parties to a business transaction as stated in ISO/IEC 15944-1:—, 6.2.6 apply (see B.3).

Rule 095:

Any delegation by a seller, buyer and/or regulator of any aspect of the instantiation of a business transaction to an agent or third party shall include identification of applicable ILCM requirements and, in particular, applicable personal information requirements.

Rule 096:

Where the delegation by a seller or regulator of any aspect of the instantiation of a business transaction involves an individual as buyer, the organization or public administration in its role as a seller (or regulator) shall ensure that such delegation is conformant with applicable external constraints of the jurisdictional domain of the location of the buyer, as an individual:

a) **pertaining to whether or not the specific role or sub-role(s) can be delegated in the first place depending on the good, service and/or right being provided; and**

b) **ensuring that the individual provides explicit and informed consent with respect to such a delegation by the seller to an agent or third party.**

29) A key aspect of "blockchain" business transactions is that they provide (100 %) transactional integrity, and thus where a blockchain business transaction contains personal information (Pi) it is able to be constructed to provide (100 %) PPTI.

Rule 097:

Irrespective of the location of the SRIs/SPIs pertaining to a business transaction and the use of agents and/or third parties, the organization that is the seller is, and remains, solely and uniquely responsible for ensuring privacy protection for personal information including all associated ILCM requirements.

10.2 ILCM rules pertaining to use of an "agent"

A seller should not interchange SPIs with its agent(s) unless the agent has in place procedures and mechanisms which support privacy protection requirements (PPR).

Rule 098:

Where a seller uses an agent, the seller shall ensure before interchanging any personal information (PI) with an agent (and its IT system), that the agent (and its IT systems) support applicable privacy protection requirements.

This is essential for the seller to be compliant with PPRs when the buyer is an individual., i.e., the seller may not interchange PI with another organization, including its agent(s), unless the agent is also in compliance with applicable privacy requirements.

Guideline 098G1:

Prior to an organization delegating part (or all) of the instantiation of a business transaction to an agent via EDI, the organization 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. This includes the agent having a designated privacy protection officer (PPO) and a personal information controller (PIC).

Rule 099:

Where a state change occurs to personal information pertaining to a business transaction, and the seller has interchanged such personal information to its agent(s), the seller shall notify the agent of such a state change(s) and the agent shall acknowledge receipt of the same and verify that it has made the same state change in its IT systems.

Rule 100:

Where a seller uses an agent and interchanges personal information pertaining to a business transaction, the seller shall ensure that the agent in its IT systems supports applicable records retention and disposal scheduling of that personal information.

Guideline 100G1:

A seller can ensure that records retention and disposal requirements pertaining to personal information of a seller in a business transaction are maintained by its agent(s) through the use of state changes.

For example, when the seller destroys (i.e., expunges) the personal information as required pertaining to a specified business transaction, the seller could send a state change whereby the SCs (and IBs) pertaining to that business transaction would be changed in their content value to "00".

Rule 101:

At the completion of a business transaction, where the buyer is an individual and the seller does not dispose of all related SPIs but instead transfers those SPIs to an archive for added temporal or permanent retention, the seller shall inform the individual of the same along with (new) access and use provisions which may apply and, where applicable, the name and coordinates of the agent, i.e., another party.

10.3 ILCM rules pertaining to use of a "third party"

While the rules and guidelines in 10.3 may seem similar to those in 10.2, the crucial difference is that the role and actions of an "agent" are solely under the control of the seller, while the role and actions of a "third party" are on behalf of both the buyer and seller, as mutually agreed to by them both.

Rule 102:

Where a seller uses a third party, the seller shall ensure before interchanging any personal information with a third party (and its IT system), that the agent (and its IT systems) support applicable privacy protection requirements.

A seller should not interchange IBs or SCs with a third party unless the third party has in place procedures and mechanisms which support privacy protection requirements.

Rule 103:

Where a state change occurs to personal information pertaining to a business transaction, and the seller has interchanged such personal information to its third party(ies), the seller shall notify the agent of such a state change(s) and the third party shall acknowledge receipt of the same and verify that it has made the same state change in its IT systems.

Rule 104:

Where a seller uses a third party and interchanges personal information pertaining to a business transaction, the seller shall ensure that the third party in its IT systems supports applicable records retention and disposal scheduling of that personal information.

Guideline 104G1:

A seller can ensure that records retention and disposal requirements pertaining to personal information of a seller in a business transaction are maintained by its third party(ies) through the use of state changes.

For example, when the seller destroys (i.e., expunges) the personal information as required pertaining to a specified business transaction, the seller could send a state change whereby the SCs (and IBs) pertaining to that business transaction would be changed in their content value to "000".

Rule 105:

At the completion of a business transaction, where the buyer is an individual and the seller does not dispose of all related SPIs but instead transfers those SPIs to an archive for add temporal or permanent retention, the seller shall inform the individual of the same along with (new) access and use provisions which may apply and, where applicable, the name and coordinates of the third party, i.e., another party, rather than by the organization itself.

10.4 ILCM rules pertaining to involvement of a "regulator"

It may be that, in addition to the involvement of third party(ies), as mutually agreed by the buyer and the seller, external constraints applicable to a business transaction require the participation of a "regulator" depending on the nature of the good, service and/or right which is the goal of that business transaction. This may well introduce ILCM-related requirements as external constraints of the regulator.

Rule 106:

Where the nature of the business transaction requires the participation of EDI with a regulator (and its IT systems), the seller shall ensure that the regulator (and its IT system(s)) support applicable PPR.

A seller should not interchange IBs or SCs with a regulator unless the regulator has in place procedures and mechanisms which support privacy protection requirements.

Rule 107:

Where a state change occurs to personal information pertaining to a business transaction, and the seller has interchanged such personal information to a regulator(s), the seller shall notify the regulator of such a state change(s) and the regulator shall acknowledge receipt of the same and verify that it has made the same state change in its IT systems.

Rule 108:

Where a seller uses a regulator and interchanges personal information pertaining to a business transaction, the seller shall ensure that the regulator in its IT systems supports applicable records retention and disposal scheduling of that personal information.

Guideline 108G1:

A seller can ensure that records retention and disposal requirements pertaining to personal information of an individual in a business transaction are maintained by the regulator(s) through the use of state changes.

For example, when the seller destroys (i.e., expunges) the personal information as required pertaining to a specified business transaction, the seller could send a state change whereby the SCs (and IBs) pertaining to that business transaction would be changed in their content value to "000".

It is assumed that a regulator is involved in EDI pertaining to a business transaction due to applicable external constraints which require some or all of the SRIs pertaining to the business transaction to be interchanged with the regulator by the seller.

11 Conformance statement

11.1 Overview

The first two types of conformance statements presented in this clause are at the most primitive level only.

This clause is modelled on that found in ISO/IEC 14662:2010, Clause 6.

There are two different categories of conformance statements for this document:

a) Category A — ISO/IEC 14662 Open-edi reference model; and, ISO/IEC 15944 compliance; and

b) Category B — ISO/IEC 15944-12 conformance only. These basically apply for use by a seller or regulator.

The reason for these two categories is to permit users and implementers of ISO/IEC 15944-8 to be conformant to its requirements without using the Open-edi modelling constructs as well as registration of Open-edi scenario(s) (OeS) and scenario components as re-usable business objects.

In addition, there are conformance statements for use by "agents" and "third parties" (see 11.4).

11.2 Conformance to the ISO/IEC 14662 Open-edi reference model and the ISO/IEC 15944 series

Rule 109:

Any user/implementer conformance statement of this nature shall state: (a) that it is conformant to the BOV class of ISO/IEC 14662; (b) the list of the basic concepts of the ISO/IEC *Open-edi reference model* and the ISO/IEC 15944 series as stated in ISO/IEC 15944-7; and (c) whether or not it has any Open-edi compliant scenarios and scenario components registered using ISO/IEC 15944-2.

11.3 Conformance to ISO/IEC 15944-12

Rule 110:

Any user/implementer conformance statement of this nature shall state: "*The existence, management, use and/or interchange of personal information (i.e., as SPIs) by XYZ [insert name of organization or public administration] with any other party (to the business transaction) is conformant and consistent with the eleven privacy protection principles and associated information life cycle management (ILCM) requirements as stated in the definitions, concepts, rules, guidelines and related requirements of ISO/IEC 15944-12*".

11.4 Conformance by agents and third parties to ISO/IEC 15944-12

It is the seller in a business transaction who is responsible for ILCM of personal information pertaining to a business transaction where the buyer is an individual.

This means personal information maintained under the control of the organization acting in the role of seller, including as ILCM of the organizations' IT systems (and related DMAs). Where and when an (seller) organization decides to use an agent or a third party in the fulfilment of a business transaction containing personal information, the seller organization shall ensure that any agent or third party with which it interchanges personal information is "conformant" with ISO/IEC 15944-12.

Rule 111

An organization, in the role of seller, in a business transaction where the buyer is an individual and the business transaction contains personal information shall ensure before interchanges of any such personal information occur with an agent or third party that such an agent or third party is conformant with applicable privacy protection requirements.

Conformance statement for use by parties who function as agents or third parties to a seller organization in a business transaction where the buyer is an individual and the business transaction involves personal information.

> *"Organization "XYZ" [insert name of organization] acting as an agent or third party [indicate which] to organization "ABC" [insert name of organization acting as the seller in a business transaction] hereby states that it is conformant in its IT systems with respect to the content value(s) of any and all SPIs pertaining any EDI of such SPIs with the eleven privacy protection principles and associated information life cycle management (ILCM) requirements as stated as in the definitions, concepts, rules and related requirements of ISO/IEC 15944-12. This includes organization "XYZ" having a designated role/function of privacy protection officer (PPO) and personal information controller (PIC) as an organization person(s)."*

Annex A
(normative)

Consolidated list of terms and definitions with cultural adaptability: ISO English and ISO French language equivalency

A.1 Purpose

All parts of the ISO/IEC 15944 series maximize the use of existing standards where and whenever possible including relevant and applicable existing terms and definitions. These are presented in Clause 3. This annex contains only those new concepts and their definitions introduced in this document, i.e. as ISO English and ISO French language HIEs.

ISO/IEC 15944-7:2009, Annex D already contains the consolidated ISO English and ISO French language equivalents for all the other concepts and definitions found in Clause 3. ISO/IEC 15944-7 also contains ISO Russian and ISO Chinese language HIEs for all the concepts and their definitions.

A.2 ISO English and ISO French

This document recognizes that the use of English and French as natural languages is not uniform or harmonized globally as this is the nature of any natural language. For example, there different variations in the spellings of the same words in the English language (and in some cases in the French language). Other examples include use of Arabic, German, Portuguese, Russian, Spanish, etc., as natural languages let alone as "official languages" (see ISO/IEC 15944-5:2008, 6.2.3) in different jurisdictional domains at various levels, including those of provinces, states, cantons, länder, etc.

Consequently, the terms "ISO English" and "ISO French" are used to indicate ISO/IEC's specialized use of English and French as natural languages in the specific context of international standardization, i.e., as a "special language". In addition, international standards often contain terms (and words) which are not (yet) found in natural language dictionaries. **As such, the variant use of the English and French language in this document is referred to as "ISO English" and "ISO French".**[30)]

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 provided in more than one language[31)](in addition to "ISO English").

This annex supports "cultural adaptability" by ensuring that, if a 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.

30) The same approach is taken in ISO/IEC 15944-7 which, in addition to ISO English and ISO French equivalencies for definitions and associated terms, also does so in ISO Russian and ISO Chinese.

31) Many of the ISO/IEC JTC1 standards pertain to "programming languages" (e.g., Fortran, C++, Java, etc.) or "markup" languages e.g., SGML or its derivative XML). These are not "natural" or "special" languages and thus do not have multilingual equivalents.

Translating terms and definitions:

— Adds a level of a "quality control check" in that establishing an equivalency in another language identifies ambiguities in the source language.[32)]

— Recognizes that in languages other than English, the grammatical gender of the term is important as the same word, i.e., character string may have a completely different meaning depending on its grammatical gender (see ISO/IEC 15944-5:2008, 6.2.6).

— Enhances the widespread adoption and use of standards worldwide, especially by users of this document who include various industry sectors, different legal perspective, policymakers and consumer representatives, other standards developers, IT hardware and service providers, etc.

— Takes an IT-enabled approach which promotes interoperability from both IT and human interface perspectives (see ISO/IEC 15944-5). An essential aspect of this approach is to use the unique and unambiguous composite identifier of each term/definition pair as the ID code with which are associated multiple bilingual/multilingual textual equivalent representations.

A.4 Organization of Annex A — Consolidated list in matrix form

The terms/definitions are organized in matrix form in alphabetical order (English language). The columns in the matrix are as follows:

Table A.1 — Columns in Table A.2

Col. No.	Use
	IT-interface — Identification
1	eBusiness vocabulary ID (as assigned in ISO/IEC 15944-7)[a]
2	Source. International standard referenced or that of ISO/IEC 15944-12 itself
	Human interface equivalent (HIE) components
3	ISO English language — term
4	Gender of ISO English language term[b]
5	ISO English language — definition
6	ISO French language — term [c]
7	Gender of the ISO French language term[b]
8	ISO French language — definition

[a] eBusiness Vocabulary IDs are assigned based on the next available Dnnn sequential number.

[b] The codes representing gender of terms in natural languages are found in ISO/IEC 15944-5:2012, 6.2.6 and Table 1 (they are "01 = masculine/masculine", "02 = feminine/feminine", and "03 = neuter/neutre").

[c] The use of French language equivalents, required in Column (8), means that these also serve as inputs into ISO/IEC 15944-7:2009, Annex D.

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 (see ISO/IEC 15944-7).

A.5 List of newly introduced in Part 12 terms and definitions with cultural adaptability: ISO English and ISO French

32) No quality management system standards exist pertaining to the quality, integrity and unambiguity of the "data" or "data element" itself, let alone unambiguity in its semantics. However, ISO/IEC 20016-1 does address and resolve many of these issues.

Table A.2 — List of newly introduced terms and definitions with cultural adaptability of: ISO English and ISO French language equivalency

IT-interface		Human interface equivalent (HIE) components					
Identification		ISO English			ISO French		
eBus. vocabID	Source ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
D308	ISO/IEC 15944-12:2019, 3.6	back-up copy of data	99	copy that is any of the following: (a) additional resource or duplicate copy of **data** on different a storage **medium** stored off-line for emergency purposes; (b) disk, tape or other machine-readable copy of a **data** or program file; (c) **data** or program file recorded and stored off-line for emergency or archival purposes; and, (d) record that preserves the evidence and information it contains if the original is not available	copie de sécurité de données	02	copie de toute nature suivante : (a) ressource supplémentaire ou copie double de **données** sur un **support** de **données** stocké hors-ligne en cas d'urgence; (b) disque, ruban ou autre copie de **données** ou fichier de programmes lisible par machine; (c) **données** ou fichier de programmes enregistré et stocké hors-ligne en cas d'urgence ou d'archivage; et, (d) enregistrement qui préserve la preuve et l'information qu'il contient si l'original n'est pas disponible
D309	ISO/IEC 15944-12:2019, 3.11	business transaction audit trail	99	chronological record of **IT system** activities that is sufficient to enable the reconstruction, reviewing and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event pertaining to **sets of recorded information (SRIs)** in a **business transaction** through all its **processes**, i.e., from **planning** to the end of **post-actualization** Note to entry: The ability to support a business transaction audit trail is required in order to be able to support privacy protection transactional integrity (PPTI) requirements.	piste de vérification de transaction d'affaires	02	enregistrement chronologique des activités d'un **système TI** suffisant pour permettre la reconstruction, la révision et l'examen de la séquence d'environnements et d'activités entourant (ou menant à) une opération, une procédure, ou un événement relatif à des **ensembles d'information enregistrée (SRI)** dans une **transaction d'affaires** à travers tous ses **processus**, c.-à.-d. de la **planification** jusqu'à la fin de la **post-actualisation** Note à l'article: La capacité de soutenir la piste de vérification d'une transaction d'affaires est exigée pour soutenir les exigences de l'intégrité transactionnelle de la protection de la vie privée (PPTI).
D319	ISO/IEC 15944-12:2019, 3.25	consumer information profile (CIP)	99	any one or more, **personal information profiles (PIPs)** and any related **personal information** on or about an identifiable **individual** to which **consumer protection** requirements apply, i.e., in addition to applicable **privacy protection** requirements	profil d'information du consommateur (CIP)	01	tout (ou plusieurs) **profil d'information personnelle (PIP)** et toute **renseignements personnels** connexe sur (ou à propos d') un **individu** identifiable auquel s'appliquent des exigences de **protection du consommateur**, c.-à.-d. en plus des exigences de **protection de la vie privée** applicables

Table A.2 *(continued)*

IT-interface		Human interface equivalent (HIE) components					
Identification		ISO English			ISO French		
eBus. vocabID	Source ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
D311	ISO/IEC 15944-12:2019, 3.30	data back-up	99	**process** of duplicating and archiving **data,** often on a different storage **medium,** so that it may be restored to its original state after a data loss event Note 1 to entry: The primary purpose of "back-up" is to recover data be it by data deletion or corruption. Note 2 to entry: A secondary purpose of back-up is to be able to recover data from an earlier time according to a predefined retention policy.	sauvegarde de données	02	**processus** de duplication et d'archivage de **données**, souvent sur un **support** de stockage différent, afin de pouvoir les restaurer à leur état original après une perte de données Note 1 à l'article: Le but principal de la sauvegarde est de récupérer les données d'un moment antérieur selon une politique de rétention prédéfinie. Note 2 à l'article: Un but secondaire de la sauvegarde est de pouvoir récupérer les données d'un moment antérieur selon une politique de rétention prédéfinie.
D312	ISO/IEC 15944-12:2019, 3.31	data conversion	99	**process** of changing **data**, i.e., as **set(s) of recorded information (SRI(s)),** from one format or representation to another while maintaining the **characteristics** of the **SRIs** including the authenticity, integrity, reliability and usability of the **sets of recorded information (SRI(s))** as well as relevant **information life cycle management (ILCM)** requirements, and especially those of an **external constraints** nature including **privacy protection** requirements where the **data** involves **personal information** Note 1 to entry: A characteristics of data conversion is a change in the format used for managing and/or representing the contents of the SRI.	conversion de données	02	**processus** de changer des **données**, c.-à.-d. un (ou des) **ensemble(s) d'information enregistrée** (SRI(s)), sous un format (ou une représentation) en un autre, tout en conservant les **caractéristiques** de la **SRI**, y compris l'authenticité, l'intégrité, la fiabilité et l'utilisabilité des **ensembles d'information enregistrée (SRIs),** ainsi que les exigences applicables à la **gestion du cycle de vie de l'information (ILCM)**, et particulièrement celles de nature de **contraintes externes**, y compris les exigences de **protection de la vie privée** lorsque les **données** contiennent des **renseignements personnels** Note 1 à l'article: Une des caractéristiques de la conversion de données est le changement de format utilisé pour gérer et/ou représenter le contenu de la (des) SRI(s).

Table A.2 *(continued)*

IT-interface		Human interface equivalent (HIE) components					
Identification		ISO English			ISO French		
eBus. vocabID	Source ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				EXAMPLE Data conversion resulting from a change in text processing software (e.g. MS Word to HTML), from one database software to another, from a non-data based software to a database based software approach or vice-versa, etc. Note 2 to entry: A data conversion does not change the content value of the SRI(s). [SOURCE: Adapted from CAN/CGSB-72.34-2005, 3.16 and ISO 13008:2012, 3.5.]			EXEMPLE La conversion de données résultant d'un changement de logiciel de traitement de texte (par ex. de MS Word à HTML), d'un logiciel de base de données à un autre, d'un logiciel non basé sur des données à un logiciel de base de données ou vice-versa, etc. Note 2 à l'article: Une conversion de données ne change pas la valeur du contenu d'une (ou des) SRI(s). [SOURCE: Adapté de CAN/CGSB-72.34-2005, 3.16 et ISO 13008:2012, 3.5.]
D313	ISO/IEC 15944-12:2019, 3.33	data migration	99	**process** of moving **data**, i.e., as **sets of recorded information (SRIs)** including their existing **characteristics** from one **IT System**, (e.g., hardware or software configuration) to another, as required by changes in an **IT System** configuration or as requested by the user, while assuring that the **SRI(s)** will remain addressable and that data authenticity, integrity, reliability and useability of the **SRI(s)** will be maintained in the new environment Note to entry: Data migration does not change the content of the SRIs. [SOURCE: Adapted from ISO 13008:2012, 3.12.]	migration de données	02	**processus** de déplacer des **données**, c.-à.-d. comme **ensembles d'information enregistrée (SRI(s))**, y compris leurs **caractéristiques** existantes, d'un **système TI** (par ex. une configuration matérielle ou logicielle) à un autre, tel qu'exigé suite à des changements de configuration d'un **système TI** ou à la demande de l'utilisateur, tout en s'assurant que le (ou les) **SRI** reste adressable et que l'authenticité des données, l'intégrité, la fiabilité et l'utilisabilité de la (ou les) **SRI** seront préservées dans le nouvel environnement Note à l'article: La migration de données ne change pas le contenu des SRI. [SOURCE: Adapté de l'ISO 13008:2012, 3.12.]

Table A.2 *(continued)*

IT-interface		Human interface equivalent (HIE) components					
Identification		ISO English			ISO French		
eBus. vocabID	Source ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
D314	ISO/IEC 15944-12:2019, 3.42	electronic signature	99	signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with a particular digital/electronic **set of recorded information (SRI)** Note to entry: A Person signature may be in the form of an electronic signature or not. [SOURCE: ISO/IEC 15944-12:2019, 3.39. Adapted from PIPEDA, Part 2, section 31(1); CAN/CGSB-72.34-2005, 3.28.]	signature électronique	02	signature qui consiste en une ou plusieurs lettres, caractères, chiffres ou autres symboles sous forme numérique, et incorporée dans, jointe à, ou associée à un **ensemble d'information enregistrée (SRI)** Note à l'article: Une signature de Personne peut être sous forme de signature électronique ou non. SOURCE: ISO/IEC 15944-12:2019, 3.39. Adaptée de PIPEDA, Partie 2, section 31(1); CAN/CGSB-72.34-2005, 3.28.]
D315	ISO/IEC 15944-12:2019, 3.44	expungement	99	**process** of ensuring complete elimination, wiping out, destroying, or obliteration of any **recorded information** (or **sets of recorded information (SRIs)**), often including the **medium** on which it is recorded, so that there can be no reconstruction of any its contents in whole or in part	radiation	02	**processus** de s'assurer de l'élimination, de la suppression, de la destruction ou de l'oblitération complète de toute **information enregistrée** ou d'un (ou de) ensemble(s) **d'information enregistrée(s) (SRI(s))**, incluant souvent le **support** sur lequel elle est enregistrée, afin qu'il ne puisse y avoir aucune reconstruction totale ou partielle de n'importe quelle partie de son contenu
D316	ISO/IEC 15944-12:2019, 3.58	information life cycle management (ILCM)	99	series of actions and **rules** governing the management and its **electronic data interchange (EDI)** of **set(s) of recorded information (SRIs) under the control of** a **Person** from its creation to final disposition in compliance with applicable **information law** requirements Note to entry: The inclusion of information law brings into this definition all the various information management activities.	gestion du cycle de vie de l'information (ILCM)	02	série d'action et de **règles** gouvernant la gestion et son **échange de données informatisées (EDI)** d'un (ou de) ensemble(s) **d'information enregistrée(s) (SRI(s)) sous le contrôle d'une Personne**, de sa création jusqu'à la disposition finale, conformément aux exigences du **droit de l'information** Note à l'article: L'inclusion du droit de l'information introduit dans cette définition toutes les différentes activités de gestion de l'information.

Table A.2 *(continued)*

IT-interface		Human interface equivalent (HIE) components					
Identification		ISO English			ISO French		
eBus. vocabID	Source ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
D317	ISO/IEC 15944-12:2019, 3.91	personal information controller (PIC)	99	**organization Person** authorized and so formally designated by the **organization** to ensure that **personal information** remains (fully) **under the control of** the **organization** and ensures its **privacy protection transactional integrity (PPTI)** in compliance with applicable **privacy protection** requirements including in any use by the **organization** of **agents** and/or **third parties** in support of a **business transaction(s)** Note 1 to entry: The primary role and responsibility pertain to and focus on ensuring that (a) personal information remains "under the control of" the organization; and, (b) required ILCM aspects are implemented in a verifiable manner. A PIC also bridges the BOV-to-FSV with respect to all aspects of information handling (processing and EDI) of personal information of IT system(s) in an organization.	contrôleur de l'information personnelle (PIC)	01	**Personne d'organisation** autorisée et nommée officiellement par l'**organisation** afin d'assurer que les **renseignement personnels** reste (entièrement) **sous le contrôle de** l'organisation, et d'assurer son l'intégrité transactionnelle de la vie privée (PPTI) conformément aux exigences de **protection de la vie privée** applicables, y compris dans n'importe quelle utilisation par l'**organisation** d'**agents** et/ou de **tierces parties** à l'appui d'une (ou de) **transaction(s) d'affaires** Note 1 à l'article: Le rôle et la responsabilité principaux visent essentiellement à s'assurer que (a) un (ou des) renseignements personnels reste «sous le contrôle de» l'organisation; et que (b) les aspects de l'ILCM exigés sont appliqués de façon vérifiable. Un PIC établit également une liaison BOV/FSV en ce qui concerne tous les aspects de la manipulation (traitement et EDI) de l'information personnelle dans les systèmes TI dans une organisation.

Table A.2 *(continued)*

IT-interface		Human interface equivalent (HIE) components					
Identification		ISO English			ISO French		
eBus. vocabID	Source ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				Note 2 to entry: A privacy protection officer (PPO) is a role of an officer in an organization. It may well be that the same organization Person is assigned responsibility for more than one role within an organization including those pertaining to corporate information law compliance, responsibility for corporate internal constraints such as information/records management, security, etc. Note 3 to entry: An organization may authorize and designate its privacy protection officer (PPO) to also function in the role of its personal information controller (PIC). Note 4 to entry: A PIC has a defined set of responsibilities which can be "outsourced" should a seller decide to use an agent and/or third party based on a contractual agreement to ensure that the privacy protection requirements (rights) of the buyer as an individual are fully supported.			Note 2 à l'article: Un agent de protection de la vie privée (PPO) est le rôle d'un agent dans une organisation. Il est fort possible que la même personne d'organisation se voit attribuée la responsabilité de plusieurs rôles dans une organisation, y compris ceux qui ont trait à la conformité au droit de l'information sur les sociétés, la responsabilité des contraintes internes des sociétés telles que la gestion de l'information/enregistrements, la sécurité, etc. Note 3 à l'article: Une organisation peut autoriser et nommer son agent de protection de la vie privée (PPO) pour jouer le rôle de contrôleur d'information personnelle (PIC). Note 4 à l'article: Un PIC a une série définie de responsabilités qui peuvent être «externalisées» au cas où un fournisseur décide d'utiliser un agent et/ou un tiers basé sur un accord contractuel pour s'assurer que les exigences (ou droits) de protection de la vie privée de l'acheteur à titre d'individu sont entièrement respectées.

Table A.2 *(continued)*

IT-interface		Human interface equivalent (HIE) components					
Identification		ISO English			ISO French		
eBus. vocabID	Source ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
D318	ISO/IEC 15944-12:2019, 3.92	personal information profile (PIP)	99	any collection of **personal information (PI)** or aggregation of **sets of personal information (SPIs)** including associated **identifiers**, linkages and/or associations, on or about an identifiable **individual** being collected, retained, managed, used, etc., by any other **Person** and in particular an **organization or public administration** and as such to which **privacy protection** requirements apply including those of a **ILCM** nature Note 1 to entry: A personal information profile (PIP) includes any personal information (PI) created by the seller (and parties acting on its behalf such as an agent) in the instantiated business transaction, (e.g., in the post-actualization phase assigning an applicable warranty for the good, service and/or right purchased to another individual where the original buyer (as an individual) "gifts" the good to another individual.	profil de renseignement personnel (PIP)	01	toute collecte de **renseignement personnels (PI)** ou agrégation d'**ensemble d'information personnelle (SPI)**, y compris les **identificateurs**, liens et/ou associations connexes, sur (ou à propos) d'un **individu** identifiable, qui est recueillie, conservée, gérée, utilisée, etc., par toute autre **Personne,** et en particulier une **organisation ou administration publique**, et, en tant que telle, à laquelle s'appliquent des exigences de **protection de la vie privée**, y compris celles de nature **ILCM** Note 1 à l'article: Un profil d'information personnelle (PIP) inclut toute renseignements personnels (PI) créée par le fournisseur (et les parties agissant en son nom, tel qu'un agent) dans une transaction d'affaires instanciée, (c.-.à.-d. dans la phase de post-actualisation attribuant une garantie applicable au produit, au service et/ou au droit acheté à un autre individu lorsque l'acheteur original (à titre d'individu) «fait présent» du bien à un autre individu.
				Note 2 to entry: A personal information profile (PIP) often includes personal information (PI) resulting from more than one instantiated business transaction.			Note 2 à l'article: Un profil d'information personnelle (PIP) inclut souvent des renseignements personnels (IP) résultant de plusieurs transactions d'affaires instanciées.

Table A.2 *(continued)*

IT-interface		Human interface equivalent (HIE) components					
Identification		ISO English			ISO French		
eBus. vocabID	Source ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
D319	ISO/IEC 15944-12:2019, 3.99	privacy protection transactional integrity (PPTI)		**process** of ensuring that the **seller** ensures that **data synchronization** requirements among the **IT systems** of all **parties** to a **business transaction** conform to, and are compliant with, applicable **privacy protection** requirements (PPR) of (all) the **jurisdictional domain(s)** applicable to that instantiated **business transaction** where and whenever such a **business transaction** involves a **buyer** as an **individual**, i.e., whenever any part of the **recorded information** of that **business transaction** involves **personal information (PI)** Note to entry: The concept and requirement of transactional integrity which focuses on EDI among IT systems is based on the requirements for referential integrity within an IT system of an organization.	intégrité transactionnelle de la protection de la vie privée (PPTI).	02	**processus** de s'assurer que le **fournisseur** vérifie que les exigences de **synchronisation des données** dans les **systèmes TI** de toutes les parties dans une **transaction d'affaires** se conforment aux exigences de **protection de la vie privée** (PPR) dans tous les **domaines juridictionnels** applicables à cette **transaction d'affaires** instanciée au lieu et au moment où une telle **transaction d'affaires** implique un **acheteur** à titre d'**individu**, c.-à.-d.au moment où toute partie de l'**information enregistrée** de cette **transaction d'affaires** implique de l'**information personnelle (PI)** Note à l'article: Le concept et l'exigence de l'intégrité transactionnelle axés sur l'EDI entre les systèmes IT est basés sur les exigences de l'intégrité référentielle dans un système TI d'une organisation.
D320	ISO/IEC 15944-12:2019, 3.127	set of personal information (SPI)	99	set of recorded information (SRI) which is of the nature of, or contains, personal information	ensemble d'information personnels (SPI)	01	ensemble d'information enregistrée (SRI) de la nature (ou qui contient) des renseignements personnels
D321	ISO/IEC 15944-12:2019, 3.131	SPI expungement	99	**process** of ensuring **expungement** of a **set of personal information (SPI)** in accordance with **privacy protection** laws and regulations of the applicable **jurisdictional domain** Note to entry: In a business transaction the seller shall ensure that all parties to the business transaction including agents, and/or third parties with whom such a set(s) of personal information was exchanged are also expunged, i.e., as part of ensuring transactional integrity.	radiation de SPI	02	**processus** d'assurer la **radiation** d'un **ensemble d'information personnelle (SPI)** conformément aux lois et règlements de **protection de la vie privée** du **domaine juridictionnel** applicable Note à l'article: Dans une transaction d'affaires, le fournisseur doit s'assurer que toutes les parties dans une transaction d'affaires, y compris les agents et/ou les tierces parties entre lesquelles une telle ensemble(s) d'information personnelle a été échangée, radie également cette même série afin d'assurer l'intégrité transactionnelle

Table A.2 *(continued)*

IT-interface		Human interface equivalent (HIE) components					
Identification		ISO English			ISO French		
eBus. vocabID	Source ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
D322	ISO/IEC 15944-12 :2019, 3.132	SRI custody	99	association between a **Person** having physical or virtual possession of a **set(s) of recorded information (SRIs)** in the **role** of an **agent** or a **third party** on behalf of the **Person** who is responsible for **under the control of** associated legal/regulatory requirements pertaining to the **SRI(s)**, in particular **privacy protection requirements (PPRs)** Note to entry: On the whole, the default is that of the SRI pertaining to any business transaction as being the Person in the role of seller for the instantiation of that business transaction.	garde de SRI	02	association entre une **Personne** ayant la possession physique ou virtuelle d'une (ou de) **série(s) d'information enregistrée (SRIs)** dans le rôle d'un **agent** ou d'une **tierce partie** au nom de la **Personne** responsable **sous le contrôle des** exigences légales/réglementaires relatives à (ou aux) **SRI(s)**, en particulier les **exigences de protection de la vie privée** Note à l'article: Dans l'ensemble, la SRI relative à toute transaction d'affaires à titre de Personne jouant le rôle de fournisseur pour l'instanciation de cette transaction d'affaires est implicite.
D323	ISO/IEC 15944-12:2019, 3.133	SRI destruction	99	**process** of eliminating or deleting a **set of recorded information**, beyond any possible reconstruction	destruction de SRI	02	processus d'élimination ou de suppression d'un ensemble d'information enregistrée (SRI)

Table A.2 *(continued)*

IT-interface		Human interface equivalent (HIE) components					
Identification		ISO English			ISO French		
eBus. vocabID	Source ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
D324	ISO/IEC 15944-12:2019, 3.134	SRI integrity	99	reliability and trustworthiness of a **set(s) of recorded information (SRI(s))**, as well as of any copies, duplicates or comparable representations of the **SRI(s)**; and reliability and trustworthiness of the **IT system(s)** in which the SRI(s) were recorded or stored to produce reliable and trustworthy copies and duplicates of **set(s) of recorded information (SRI(s))** Note 1 to entry: SRI integrity is important in the electronic records provisions of the evidence acts in the phrases "the integrity of the electronic records system" and "the integrity of the electronic record." However, the term integrity is not defined in rules governing forensic data in 'evidence acts'. In the absence of a statutory or judicially created definition, the principles of this Part 12 shall serve as an operational definition of the word "integrity" when used in the context of 'evidence acts'. Note 2 to entry: Certain evidence acts provide that the integrity of the electronic record may be proved by evidence of reliable and adequately implemented encryption.	intégrité de SRI	02	fiabilité et confiance dans une (ou des) **ensemble(s) d'information enregistrée (SRI(s))** et également en ce qui a trait aux copies, duplicata ou représentations comparables de **SRIs**, et fiabilité du (et confiance dans le) **système TI** dans lequel elle a été enregistrée ou stockée pour produire des copies et des duplicatas d'**ensembles d'information enregistrée (SRI(s))** fiables et dignes de confiance Note 1 à l'article: L'intégrité de la SRI est importante pour la disposition des enregistrements électroniques des lois sur la preuve dans les phrases «l'intégrité des systèmes d'enregistrement électroniques» et «l'intégrité de l'enregistrement électronique». Cependant, le terme «intégrité» n'est pas défini dans les lois sur la preuve. En l'absence d'une définition créée statutairement ou juridiquement, les principes de la présente Partie12 norme doivent servir comme définition opérationnelle du mot «intégrité» utilisé dans les lois sur la preuve. Note 2 à l'article: Certaines lois sur la preuve stipulent que l'intégrité de l'enregistrement électronique peut être fournie sur preuve d'un cryptage fiable.

Table A.2 *(continued)*

IT-interface		Human interface equivalent (HIE) components					
Identification		ISO English			ISO French		
eBus. vocabID	Source ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				Note 3 to entry: Organizations which implement the requirements of the rules (and associated guidelines) pertaining to records retention requirements and state changes to the content values of an SRI, as defined in this Part 12 and associated Tables 1–7 are deemed to meet basic SRI integrity requirements.			Note 3 à l'article: Les organisations qui appliquent les exigences des règles (et lignes directrices connexes) relatives aux exigences de rétention d'enregistrements et aux changements d'état des valeurs du contenu d'un SRI tel que défini dans cette Partie 12 et les tableaux connexes 1–7, sont jugés comme répondant aux exigences de base de l'intégrité d'une SRI.
D325	ISO/IEC 15944-12:2019, 3.135	SRI life cycle	99	stages in the life cycle of a **set of recorded information (SRI)** which include but are not limited to its planning, creation and organization; the receipt and capture of data; the retrieval, processing, dissemination and distribution of a **set of recorded information (SRI);** its storage, maintenance and protection; and its archival preservation or **destruction** or **expungement**	cycle de vie d'une SRI	01	étapes dans le cycle de vie d'un **ensemble d'information enregistrée (SRI)** qui incluent (mais non limité à) sa planification, sa création et son organisation, la réception et la saisie de données, l'extraction, le traitement, la dissémination et la distribution d'un **ensemble d'information enregistrée (SRI)**, son stockage, sa maintenance et sa protection, et sa préservation archiveuse ou sa **destruction** ou sa **radiation**
D326	ISO/IEC 15944-12:2019, 3.136	SRI retention period	99	specified period of time that a **set(s) of recorded information (SRI(s))** is/are kept by a **Person** in order to meet operational, legal, regulatory, fiscal or other requirements	période de rétention d'une SRI	02	période de temps spécifiée qu'un (ou des) **ensemble(s) d'information enregistrée (SRI)** est (sont) conservée(s) par une **Personne** afin de répondre à des exigences opérationnelles, légales, réglementaires, fiscales ou autres
D327	ISO/IEC 15944-12:2019, 3.140	transitory record	99	**set of recorded information (SRI)** that is required only for a very limited and specified (retention period) time to ensure the completion of a routine action or the preparation of a subsequent **set of recorded information (SRI)** Note to entry: A transitory SRI is expunged at the end of a short existence.	enregistrement transitoire	01	**ensemble d'information enregistrée (SRI)** exigée seulement pour un temps limité et spécifié (période de rétention) afin d'assurer l'achèvement d'une action de routine ou la préparation d'un **ensemble d'information enregistrée (SRI)** subséquente Note à l'article: Une SRI transitoire est radiée à la fin de sa brève existence.

Table A.2 *(continued)*

IT-interface		Human interface equivalent (HIE) components					
Identification		ISO English			ISO French		
eBus. vocabID	Source ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
D328	ISO/IEC 15944-12:2019, 3.142	under the control of	99	set of requirements on an **organization**, especially those of **external constraint** nature, i.e., **privacy protection** and related **information law** requirements, requiring full and complete **information life cycle management (ILCM)** of **personal information** as **set(s) of recorded information (SRIs)** related to the agreed upon goal of the instantiated **business transaction,** including state changes to the content of the **SRIs** with respect to their creation/collection, recording processing, organization, storage, use, retrieval, disclosure, retrieval, aggregation, dissemination, **disposition** (including **expungement**), **electronic data interchange (EDI)**, etc., and in particular that of any and all state changes in the **decision making application (DMAs)** of the **organization** and any of its **agents** and/or **third parties** (as well as any other parties) to the **business transaction**	sous le contrôle de	03	ensemble d'exigences d'une organisation, particulièrement celles de nature de **contraintes externes**, c.-à.-d. les exigences de **protection de la vie** privée et du **droit de l'information** connexes, qui exigent une **gestion du cycle de vie de l'information (ILCM)** complète et entière de la (ou des) **ensemble(s) d'information enregistrée (SRI(s))** relatif au but convenu de la **transaction d'affaires** instanciée, incluant les changements d'état apportés aux **SRIs** en ce qui concerne leur création/collecte, le traitement de l'enregistrement, l'organisation, le stockage, l'utilisation, l'extraction, l'agrégation, la dissémination, la **disposition** (y compris la **radiation**, l'**échange de données informatisé (EDI)**, etc., et en particulier celles de tout (ou tous les) changement d'état dans l'**application de prise de décision (DMA)** de l'**organisation** et de n'importe lequel de ses **agents** et/ou **tierces parties** (ainsi que n'importe quelles autres parties) à la **transaction d'affaires**

Table A.2 *(continued)*

IT-interface		Human interface equivalent (HIE) components					
Identification		ISO English			ISO French		
eBus. vocabID	Source ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				Note 1 to entry: The fact that a Person responsible for the control of a SRI(s), especially SPI(s), delegates or contracts out physical custody of the SRI(s) to an agent or third party does not take away from the responsibility of that Person for ensuring ILCM management aspects in support of privacy protection requirements remain fully supported and executed. Note 2 to entry: If and where a disposition or expungement of SPIs pertaining to a business transaction involves the transfer of the related SPIs to another organization the applicable ILCM requirements of a privacy protection nature continue to apply to the organization to which the SPIs are being transferred to.			Note 1 à l'article: Le fait qu'une personne responsable du contrôle de SRI(s) (et particulièrement de SPI(s)) délègue ou sous-traite la garde physique de la (ou des) SRI(s) à un agent ou une tierce partie, ne soustrait pas la responsabilité de cette personne de s'assurer que les aspects de gestion de l'ILCM à l'appui des exigences de protection de la vie privée, restent entièrement soutenus et exécutés. Note 2 à l'article: Si ou lorsqu'une disposition ou une radiation de SPI(s) relative à une transaction d'affaires implique le transfert de la SPI concernée à une autre organisation, la nature des exigences de protection de la vie privée de l'ILCM continue de s'appliquer à l'organisation à laquelle la (ou les) SPI(s) est transférée.

Annex B
(normative)

Consolidated set of rules in the ISO/IEC 15944 series of particular relevance to privacy protection requirements (PPR) as external constraints on business transactions which apply to personal information (PI) in an ILCM requirements context

B.1 Purpose

This document makes extensive use of rules and guidelines in ISO/IEC 15944-1 and adapts them in a privacy protection requirements context. Similarly relevant rules and guidelines in ISO/IEC 15944-2, ISO/IEC 15944-5, ISO/IEC 15944-7 and ISO/IEC 15944-8 serve as the basis for rules required to support privacy protection requirements.

The purpose of this annex is to provide a consolidated presentation of all the rules in the existing parts of ISO/IEC 15944 for the scoping and specification of Open-edi scenarios and their components which pertain to external constraints relevant to privacy protection requirements. Jurisdictional domains are the primary source of external constraints. The existing parts of the ISO/IEC 15944 series address, in an integrated manner, many of the requirements pertaining to specifying common external constraints of jurisdictional domains which are relevant to privacy protection requirements either in a generic or specific manner.

Only the rules themselves are presented here. For related text, as well as associated guidelines, where applicable, see the relevant clauses in the ISO/IEC 15944 series as identified in B.2 to B.7.

There are parts of the ISO/IEC 15944 series which do not contain any rules (or guidelines) of relevance to privacy protection requirements (PPR). These are:

1) ISO/IEC 15944-4, which focuses on "accounting and economic ontology" at the Person level as parties to a business transaction, i.e., in their roles as buyers, sellers, and/or regulators.

2) ISO/IEC TR 15944-6, which provides a technical introduction to e-Business modelling and, as such, contains no rules.

B.2 Organization of Annex B: Consolidated list in matrix form

The rules and associated references are presented in matrix form. The rules are presented in the numeric order in which they are presented in ISO/IEC 15944-1. The columns in the matrix are listed in Table B.1.

Table B.1 — Columns in Table B.2

Col. No	Use
1	Number of rule as per part of the ISO/IEC 15944 series.
2	Clause in ISO/IEC 15944-1 of which the rule is part.
3	Rule statement as per ISO/IEC 15944-1. NOTE Only text of the rule itself is presented. For associated guidelines, requirements and text see the relevant clauses in that part of the ISO/IEC 15944 series.

B.3 Consolidated list of rules in ISO/IEC 15944-1 pertaining to external constraints relevant to supporting PPR

Table B.2 — Consolidated lists of rules and associated guidelines

Rule No.	Clause ID	Rule statement
(1)	(2)	(3)
3	6.1.3	In (electronic) business transactions, all commitments shall be stated explicitly and unambiguously and be understood by all Persons involved in a business transaction.
13	6.2.2	The level of unambiguity, i.e., certainty/reliability of a persona and resulting identification of the Person identity used by a Person shall be appropriate to the goal of the business transaction.
15	6.2.2	Business transactions having different goals may allow a Person to use the same persona and its associated identification schema (including resulting identifiers), while others may prohibit this.
27	6.2.4	Unless bound by external constraints, buyers and sellers as Persons are free to undertake any business transaction involving any good, service, and/or right they mutually agree to.
28	6.2.4	External constraints governing rules and practices of buyers and sellers in business transactions apply either to Persons (undifferentiated) or distinguish among individuals, organizations, and public administrations.
29	6.2.5	Rights or obligations arising from commitments in a business transaction shall be fulfilled either directly by the Person as the end entity or by an agent acting on its behalf.
30	6.2.5	The ability to delegate a role to an agent shall be explicitly stated. If constraints shall be satisfied before such delegation can take place they shall be explicitly stated.
31	6.2.5	Where delegation of a role cannot take place this shall be explicitly stated.
32	6.2.5	A business transaction takes place between two Persons. Other Persons, i.e., third parties, may fulfil specified role(s) or functions(s) on mutual agreement or as a result of external constraints.
33	6.2.6	External constraints exist on the provisioning of goods and services and the behaviour of Persons as players in business transactions including those provided via electronic commerce.
34	6.2.7	From a minimal external constraints perspective, the three basic sub-types of Persons as role players in any business scenario are: (a) individual, (b) organization, and (c) public administration.
35	6.2.7	A legal (or artificial) Person consists of one or more natural persons and/or one or more other legal persons.
38	6.2.8	From a minimal external constraints perspective, a common set of constraints on a business transaction where the buyer is an individual are those of a consumer protection nature.
39	6.3.1	Conceptually a business transaction can be considered to be constructed from a set of fundamental phases. They are planning, identification, negotiation, actualization and post-actualization.
40	6.3.1	The five fundamental phases may take place in any order.
44	6.4.1	Electronic business transactions require recorded information.
47	6.4.2	The definition of data, and related information technology terms and definitions found in ISO/IEC 15944-1 shall able to be mapped into legal frameworks.
48	6.4.2	Standards development work in support of electronic business transactions shall incorporate and support data granularity requirements. The level of granularity reflects the degree of detail appropriate to the level of certainty required in the data being interchanged among the parties participating in a business transaction.
49	6.5.1	Open-edi scenarios and Information Bundles shall therefore be capable of reflecting constraints to be applied which may be as a result of: (a) commitments among parties, i.e., as internal constraints; and, (b) external constraints.

Table B.2 *(continued)*

Rule No.	Clause ID	Rule statement
(1)	(2)	(3)
50	7.2	The requirement for an Open-edi scenario to incorporate external constraints on a business transaction shall be stated at the outset.
51	7.2	It is necessary to state whether the Open-edi Parties in the business transaction being modelled are (a) Persons in general, i.e., undifferentiated; or (b) differentiated among categories of Persons, i.e., subtypes, as individuals, organizations and public administration.
57	7.2	If the business transaction being modelled through an Open-edi scenario (OeS) incorporates external constraints which impact FSV demands on Open-edi Support Infrastructure (OeSI), these shall be specified.
66	8.3.2.4	The OeS set of roles attribute applicable to the scenario shall be specified and referenced through their Role Identifiers.
67	8.3.2.4	One shall state which roles of the OeS are mandatory, conditional, or mandatory subject to a conditional.
68	8.3.2.4	Where applicable, constraints on the same Open-edi Party playing more than one of the roles in the set of roles applicable to the OeS shall be specified.
70	8.3.2.5	If applicable, one should state which IBs are mandatory, conditional, or mandatory subject to a conditional.
71	8.3.2.5	Where applicable, constraints on IBs pertaining to roles in the OeS shall be specified.
72	8.3.2.6	The business requirements, rules and practices applicable at the scenario level shall be specified. This specification shall be stated at a level of detail to ensure that there is no ambiguity in the commitments among Open-edi parties at the scenario level.
73	8.3.2.6	Business constraints, if any at the scenario level, pertaining to Open-edi parties and scenario components shall be specified. All of these shall be accounted for in scenario components, i.e., roles and/or information bundles.
74	8.3.2.7	Requirements or constraints arising from applicable laws or regulations at the scenario level shall be explicitly stated including the source jurisdictional domains.
75	8.3.2.7	Where multiple laws and regulations apply at the scenario level, the constraints applicable shall be integrated.
101	8.4.2.5	Constraints, if any, on an Open-edi party being able to play a role shall be specified.
103	8.4.2.7	Any external constraints arising from laws or regulations to any aspect of the role and its attributes shall be identified and stated including the reference/source of the applicable law or regulation, i.e., qualifications for a role, prescribed behaviour, restrictions on the delegation of a role, etc.
135	8.5.2.4	Any business rules controlling the content of an IB shall be identified and the nature and functioning of these rules explicitly stated. The source of such business rules shall also be referenced.
136	8.5.2.5	Any external constraints arising from laws and regulations governing the content of an IB shall be identified, the requirements explicitly stated and the source referenced.
137	8.5.2.5	Any IB created to meet a requirement of external constraints of the nature of laws and regulations should be so identified, the contents of the IB explicitly defined, at the level of granularity required, and the source law/regulation referenced.
140	8.5.2.8	Requirements for retention of recorded information for an IB, if any, shall be specified as well as which OePs involved in the associated role(s) have the primary responsibility for retaining this recorded information.
141	8.5.2.9	Requirements arising from laws or regulations for the retention of recorded information applicable to the IB, if any, shall be explicitly stated and the source(s) referenced.
146	8.5.5.1	A semantic component can be a single (simple) data element, a composite data element, or a data structure, (e.g., a set of data elements which interwork in order to ensure semantic completeness and ensure the required unambiguousness).
147	8.5.5.1	A semantic component shall be a component of at least one Information Bundle when exchanged among Open-edi Parties.

Table B.2 *(continued)*

Rule No.	Clause ID	Rule statement
(1)	(2)	(3)
153	8.5.5.2.2	A SC name is the designation of the SC ID by a linguistic expression. More than one SC name as equivalent linguistic expressions may be associated with an SC ID, (e.g., as "aliases").

B.4 Consolidated list of rules in ISO/IEC 15944-2 pertaining to external constraints of relevance to supporting PPR

Rule No.	Clause ID	Rule statement
(1)	(2)	(3)
2	5.3	The registration of any scenario or scenario component shall be capable of supporting multilingual semantic equivalents at the human interface.
3	5.3	On the while, and from an internal constraints only based perspective, parties to a business transaction are free to choose the language(s) to be used.
9	6.5	Only valid, superseded, and retired OeRIs shall be exposed when the contents of a register are made available to the public.

B.5 Consolidated list of rules in ISO/IEC 15944-5 pertaining to external constraints of relevance to supporting PPR

Rule No.	Clause ID	Rule statement
(1)	(2)	(3)
002	5.2.1	Unless a particular external constraint governing the commitment made requires that it be made in a specific jurisdictional domain, Persons are free to choose the jurisdictional domain in which the business transaction is (deemed) to take place
003	5.2.3	Depending on the nature of the goods, services or rights being provided (as the goal of the business transaction being modelled), applicable external constraints may specify and require the business transaction to be enacted in a specified jurisdictional domain.
004	5.2.3	Within a particular jurisdictional domain, it may be required to reference a specific act or regulation as well as require the participation (in some form) of a regulator.
005	5.2.3	For any business transaction (or part thereof) which involves an external constraint(s), a role of regulator(s) shall be included and modelled as part of the scenario and scenario components.
006	5.3	The primary source of a regulator having the authority to prescribe external constraints is that of a jurisdictional domain.
008	5.4	When modelling a business transaction, where one includes external constraints, it is necessary to differentiate among the three common sub-types of Person, namely individual, organization and public administration. A jurisdictional domain shall be modelled as a public administration.
016	5.7	An external constraint may specify the "explicitly shared goal" of a business transaction as a whole.
017	6.2.1	It is vital that all parties to a business transaction have a complete and unambiguous understanding, i.e., level of certainty and explicitness required, to ensure that the commitments being entered into are fully and completely understood and agreed upon by all the parties involved.

Rule No.	Clause ID	Rule statement
(1)	(2)	(3)
018	6.2.1	Persons, whether as individuals or as organization Persons acting on behalf of their organization or public administration (on whose behalf they are qualified and authorized as role players to make commitments), shall agree to the language(s) to be used in a business transaction, i.e., by all the parties involved, in order to ensure that the semantics of the commitments being entered into are completely understood by all parties involved.
019	6.2.1	Choice of use of language(s) is governed by three primary factors: 1) seller, i.e., supplier choice; 2) buyer, i.e., user, demands; and/or; 3) regulator, i.e., requirements of a jurisdictional domain.
020	6.2.1	In business transactions which are modelled and registered as scenarios and scenario components which involve internal constraints only, the parties involved are free to choose and decide among themselves the natural language(s) to be used for the recorded information in a business transaction.
021	6.2.1	In modelling a business transaction which involves internal constraints only, it is advisable that parties concerned use the 3-alpha language code set as stated in ISO 639-2 for the identification of the language(s) to be used and/or supported.
022	6.2.2	In business transactions which are modelled (and registered) as scenarios and scenario components, i.e., as business objects, which involve external constraints, one shall specify the official language(s) to be supported based on the requirements of the jurisdictional domain(s) which is the source(s) for these external constraints.
023	6.2.2	In modelling a business transaction (or parts thereof) and registering them as re-useable business objects involving external constraints, these shall be modelled in a manner which supports the language requirements, including a multilingual approach, of the source of such external constraint(s), (e.g., jurisdictional domain(s)).
024	6.2.2	A jurisdictional domain has either an official language(s) or a de facto language.
025	6.2.2	It is for a jurisdictional domain to decide whether or not it has an official language. If not, it will have a de facto language.
026	6.2.2	A law or regulation of a jurisdictional domain may require the use of or the ability to support a specific language within a particular context, i.e., as a legally recognized language (LRL).
027	6.2.3	Where a jurisdictional domain has more than one official language, Persons as suppliers shall be capable of communicating with buyers (particularly as individuals) in any one of the official languages of that jurisdictional domain.
028	6.2.4	A jurisdictional domain may have either one or more official languages and, if not, may have only one de facto language.
029	6.2.6	In order to be able to specify the grammatical gender of a noun or term used as may be required based on the official (or de facto) language used, the set of "Codes Representing Gender in Natural Languages" shall be used in the modelling of a business transaction and registration of any related business object.
030	6.2.6	Where the official language (or de facto language) of a jurisdictional domain has no gender this shall be stated.
031	6.2.7	Where a jurisdictional domain has more than one official language, human interface equivalents (HIEs) are required in each official language in order to ensure unambiguity in the semantics of the commitments made.
032	6.2.7	It is up to a jurisdictional domain to establish HIEs in its official language(s) where these are part of the specification and implementation of external constraints.
033	6.2.8	In order to ensure unambiguity in the use of a natural language in business transactions it is necessary to specify the jurisdictional domain for the varied forms of that natural language to be used using common standard default conventions for the unambiguous identification, interworkings and referencing of combinations of codes representing countries, language and currencies.

Rule No.	Clause ID	Rule statement
(1)	(2)	(3)
034	6.2.8	In modelling a business transaction through scenarios and scenario components which involve external constraints and for which the source authority is a UN member state (or an administrative sub-division of the same), it is advisable that all parties concerned use the 3-digit numeric country code plus the 3-alpha language code, and in this order.
035	6.2.9	The official language of a treaty-based international organization recognized as having primary competence in a specific sector can override the official language requirements of the jurisdictional domains of UN member states.
036	6.2.9	In modelling a business transaction (or parts thereof) as scenarios and scenario components, and registering them as re-useable business objects involving internal constraints, these should be modelled in a manner which supports the language(s) of the source authorities referenced and used in such referenced specifications.
038	6.3.2	Where the buyer is an individual, the seller shall ascertain that the individual has the age qualification required by the jurisdictional domain to be able to be involved in and make commitments pertaining to the good, service and/or right being offered in the proposed business transaction.
039	6.3.2	A seller shall ensure that where its intends to sell a 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.
041	6.4	When an external constraint of a jurisdictional domain requires use of a specific identification system with respect to a recognized Person identity (rPi) and/or with respect to a good, service and/or right, pertaining to the business transaction being modelled as scenarios and scenario components as re-useable business objects, such modelling shall be done in a manner which supports the requirement of the identification system referenced.
043	6.5	Where a classification system uses identifiers for each distinct entry, (with the associated semantics in that classification system), such identifiers (or "composite identifiers") shall be used as well as their structure in modelling a scenario or scenario component.
044	6.6.2.2	Any external constraint of a jurisdictional domain which governs, limits or qualifies a Person, a Person sub-type, any role qualification, etc., with respect to a business transaction of a particular nature shall be specified unambiguously and in a manner so as to be able to be modelled using an OeDT.
046	6.6.2.3	The formation of a LRN of an incorporated organization, i.e., a legal person, is governed by the rules of the jurisdictional domain in which it is incorporated, registered and recognized as such.
047	6.6.2.3	The establishment and representation of name(s) of a public administration, i.e., its personae, is determined by the jurisdictional domain of which it is part.
048	6.6.2.3	The personae of an individual shall include at least one LRN in order to confirm the existence of that individual as a "natural person," i.e., the birth certificate name (or a similar name).
049	6.6.2.3	The establishment and representation of an individual, i.e., its personae, is determined by the role and context of that individual within a jurisdictional domain, i.e., as controlled by a regulator and the associated public administration.
052	6.6.3	A Person may terminate a business transaction by any agreed method of conclusion.
054	6.6.4.3	An instantiated business transaction shall have one or more IB or SC for which no state changes are permitted. One of these is to serve as the transaction ID number, i.e., a business transaction identifier (BTI), for the instantiated business transaction.
055	6.6.4.5	In the modelling of a business transaction, through a scenario and scenario components, and/or registering them as referenceable and reusable business objects, one shall specify the temporal schema, i.e., date/time referencing system, if one is used as well as the level of granularity supported.
056	6.6.4.5	Any calendar, date/time referenced, etc., identified and referenced shall be one based on (or linkable to) an ISO 8601 series or ISO 19108 and conformant to the requirements of either one of these two standards.

Rule No.	Clause ID	Rule statement
(1)	(2)	(3)
057	66.4	Where the Gregorian calendar is used, the ISO 8601 series compliant representation of 1) a date in a YYYY-MM-DD format; and 2) a time of day in an hh:mm:ss format, shall be used.
058	6.6.4.5	Where from an IT-system perspective and/or financial system needs perspective, a "GPS calendar clock" or an "atomic clock" is to be used, this shall be specified.
059	7.1	The basic rules for the formation and identification of jurisdictional domains are governed by the Charter of the United Nations and more specifically by the Vienna Convention on the Law of Treaties.
060	7.2	UN member states as peer jurisdictional domains are to be referenced by their 3-digit numeric code as stated by the UN statistical system.
061	7.2	Where the 3-digit numeric code of a UN member state is to be used in conjunction with, i.e. required to interwork with (1) a code representing an official (or de facto) language of that jurisdictional domain; (2) a code representing a currency recognized for use in that jurisdictional domain; and/or, (3) both (1) and (2), one shall use the standard default conventions for the identification, interworking and referencing of combinations of codes representing countries, languages and currencies as provided in Annex D.
066	7.8.2	In order to ensure unambiguous identification in referencing UN member states, the 3-digit numeric codes of the UN Statistical Division representing the UN member state shall be used as its primary identifier.
070	8.2	It is important in scoping an Open-edi Scenario (OeS) to specify at the outset whether or not external constraints apply to the business transaction being modelled.

B.6 Consolidated list of rules in ISO/IEC 15944-7 pertaining to external constraints of relevance to supporting PPR

ISO/IEC 15944-7 provides the ISO English and ISO French language equivalents, i.e., as HIEs, for all the definitions of concepts (and associated terms) found in ISO/IEC 14662, ISO/IEC 15944-1, ISO/IEC 15944-2, ISO/IEC 15944-4, and ISO/IEC TR 15944-6.

Although ISO/IEC 15944-7 is of the nature of a consolidated and integrated "controlled vocabulary (CV)", it does contain rules which are relevant from a PPR perspective. These are rules which are of the nature of supporting and assuring "unambiguity" in definitions of (key) concepts in the recorded information provided in support of a business transaction where the buyer is an individual and thus privacy protection requirements apply. These rules also support (and facilitate) the provision of HIEs in many a languages.

Finally, it is a requirement that any organization or public administration, which is subject to privacy protection requirements, shall make publicly available its privacy protection policy. As such, it is advised that any definitions in an organization's privacy protection policy apply and implement these ISO/IEC 15944-7 rules to support and ensure "unambiguity" in any definitions as well as HIE support.

Rule No.	Clause ID	Rule statement
(1)	(2)	(3)
001	5.2	The use of a rule-based and flexible object oriented approach for ISO/IEC 15944-7 requires rigorous quality and integrity control of the definitions to ensure that there is no tautology, i.e. circularity, in the full set of concepts defined in the international standard.
005	5.2	The presentation for a HIE eBusiness vocabulary shall be in a form and format as already provided in ISO/IEC 15944-7:2009, Annexes D, E or F.

Rule No.	Clause ID	Rule statement
(1)	(2)	(3)
006	5.3	The set of essential elements of each entry (or record) in the eBusiness Vocabulary, for each defined concept, consists of: a) the definition (of the concept); b) the term (representing the concept); c) the abbreviation of the concept (as applicable); d) the gender code for the term; e) the composite identifier (for the concept); and f) the internal eBusiness vocabulary identifier.
007	5.3.1	The characteristics (and their unique combination) of a (new) concept shall be identified and agreed to prior to the drafting of a definition for that concept.
008	5.3.1	In the identification of the unique combination of characteristics for a concept, one shall maximize use of those already defined in existing international standards, i.e., where and whenever applicable or relevant.
009	5.3.1	Any concept requiring a definition for the clarity of the understanding and use of the ISO/IEC JTC1 international eBusiness standards shall be included in that standard.
010	5.3.1	There shall be 1) a business case and rationale for the need to introduce a (new) concept into an international standard with its resulting definition and assigned term; and, 2) such a business case and rationale shall maximize re-use and integration of existing international standards, i.e. those of ISO, IEC, ISO/IEC and/or ITU.
011	5.3.1	The descriptive statement comprising a definition shall be clear, explicit and unambiguous and stated in the form of a single sentence.
012	5.3.1	Only a concept with a single definition shall be included and both the definition and associated term shall be stated in the singular.
013	5.3.1	Any definition of an eBusiness concept shall be developed with two or more human interface equivalencies (HIEs) in order to maximize its unambiguity and subsequent use in support of any and all commitments made among parties to a business transaction.
014	5.3.1	As stated in 5.1, a concept can consist of, i.e. inherit, one or more other concepts. Consequently, where this occurs, the definition for a concept of this nature shall explicitly support this requirement.
015	5.3.1	When a concept incorporates one or more other concepts, the terms representing these concepts shall be included in bold in the definition for that concept.
016	5.3.2	The issue of "polysemy" shall be avoided in international standards development.
017	5.3.2	The term chosen to designate a concept and its definition shall be unambiguous and not easily confused with terms representing other concepts.
018	5.3.2	The fact that the primary use of the eBusiness vocabulary is to support the making of commitments, it is important that the term chose to designate a concept and its definition, is unambiguous and not confused with other concepts (meanings).
019	5.3.2	A term assigned to a definition of a concept is deemed to be a "noun" (or the gerundial form of a noun like "identification").
020	5.3.3	In the development of a definition for a concept, the committee responsible shall decide as to whether or not an abbreviation or acronym needs to be assigned to the definition of a concept in addition to the term.
021	5.3.4	The gender of each term, as a noun, in the eBusiness vocabulary shall be specified using a coded domain in ISO/IEC 15944-5:2008, Table 1.
022	5.3.5	The identifier of any eBusiness vocabulary entry is of the nature of a composite identifier and shall meet the requirements of "identifier (in business transaction)".

Rule No.	Clause ID	Rule statement
(1)	(2)	(3)
023	5.3.5	The eBusiness vocabulary composite identifiers are composed of a minimum set of four discrete and mandatory data elements, consisting of: a) the source international standard reference for the vocabulary entry; b) the unique identifier assigned by international standards organization for the standards; c) document including part number where applicable; d) the date of the standard document as applicable e) the identifier of the clause number in the standards document referenced.
024	5.3.5	An eBusiness vocabulary identifier, as a composite identifier is deemed to be linguistically neutral and as such will have one or more human interface equivalents (HIEs) for the definitions and terms they represent.
027	5.4	In the development of a controlled vocabulary (CV) for an international standard, or a family of international standards (e.g. as here in the field of eBusiness), one shall maximize use (re-use) of applicable concepts already defined in existing international standards.
028	5.4	Where the term assigned to a defined concept, essential to the identification and referencing of a concept is already in use, the term shall be accompanied by the qualification, (e.g., as for "identifier (in a business transaction))".
029	6.2	The members of ISO/IEC JTC 1/SC 32, working with and through their national body standards organizations, are responsible in their jurisdictional domains for developing the human interface equivalents (HIEs) of the term/definition of a concept into the official language(s) of that jurisdictional domain as an annex to ISO/IEC 15944-7.
047	8.4	An eBusiness vocabulary Dnnn once assigned is deemed to be permanent and if retired shall not be re-assigned.
048	8.4	The definition in an eBusiness vocabulary entry, in a Clause 3, which is part of more than one document in the ISO/IEC 15944 series, shall not be changed without taking into consideration the other standards in which it is also included.

B.7 Consolidated list of rules in ISO/IEC 15944-8 pertaining to external constraints of relevance to supporting PPR

Rule No.	Clause ID	Rule statement
(1)	(2)	(3)
001	5.3	Where exceptions to the application of privacy protection principles exist, they shall be: 1) limited and proportional to meeting the objectives to which these exceptions relate; and 2) a) made known to the public; or, b) in accordance with law.
002	5.3.1	The protection of personal information shall be designed to prevent the misuse of such personal information.
003	5.3.2	An organization subject to privacy protection requirements in the jurisdictional domain (at whatever level) in which it delivers a good, service and/or rights, shall have in place implemented, enforceable policies and procedures with the proper accountability controls required to ensure its compliance with applicable privacy protection requirements.

Rule No.	Clause ID	Rule statement
(1)	(2)	(3)
004	5.3.2	An organization 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 organization's compliance with established privacy principles which, in turn, are compliant with and support the legal requirements of a privacy protection nature of the applicable jurisdictional domain(s) in which the organization operates.
005	5.3.2	Any organization to which privacy protection requirements apply shall have in place policies and practices which make it clear as to who (and where), in an enforceable and auditable manner, in their business operations is responsible for compliance with these external constraints as applicable to the conduct of business transactions where the buyer is an individual.
006	5.3.2	Where an organization, as a seller, delegates any aspect of a business transaction involving an individual , and interchanges personal information pertaining to that individual, to an "agent" (and/or "third party"), the organization shall ensure that: (1) in its arrangement with the designated agent (and/or third party), the agent (and/or third party) is fully aware of the applicable privacy protection requirements; and, (2) such parties commit themselves to support the applicable privacy protection requirements pertaining to the business transaction.
007	5.3.2	An agent (and/or third party) which commits itself to act on behalf of a Person acting as a seller in a business transaction where the buyer is an individual in a *jurisdictional* domain where privacy protection requirements apply, shall ensure that the DMA(s) in its IT system(s) is capable of supporting applicable external constraints requirements.
008	5.3.2	An organization shall ensure that in the execution of an (instantiated) business transaction, i.e., as identified by its business transaction identifier (BTI), that where these involve parties, other than the individual as a buyer, that such parties, are capable of and have implemented the requirements of the privacy protection principles.
009	5.3.3	The specified purpose(s) for which personal information is collected with respect to the (potential) goal of the business transaction shall be identified by the organization at or before the personal information is collected.
010	5.3.4	Where in a business transaction, the seller requires the buyer, as an individual, to provide personal information, the seller shall ensure that the collection and use of such personal information shall have the informed and explicit consent of the individual and that the same be directly linked to the specified goal of the business transaction (to be) entered into.
011	5.3.4	Any secondary use of personal information of the individual in a business transaction requires the explicit and informed consent of the individual.
012	5.3.4	Any use of "automatic opt-ins" shall be explicitly agreed to by the individual, i.e., as informed consent, and be recorded as such by the seller, i.e., in compliance with documentary evidentiary rules of the applicable jurisdictional domain.
013	5.3.4	Except with the explicit informed consent of the individual, 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 business transaction to which it pertains.
014	5.3.5	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 business transaction.
015	5.3.5	Any collection of personal information by the seller, or other parties to a business transaction, which pertains to a buyer as an individual in that business transaction, shall be lawful and fair.

Rule No.	Clause ID	Rule statement
(1)	(2)	(3)
016	5.3.5	An organization collecting personal information shall inform the individual concerned whether or not the personal information collected is: 1) essential to the intention of the business transaction; 2) required to be provided by the individual due to identified and specified constraints of jurisdictional domains applicable to the nature and goal of the business transaction; and/or 3) "optional", i.e., desired to have by the organization, acting as the seller, but not required.
017	5.3.6	The integrated set of ILCM principles applies to and supports the external constraints of a privacy protection nature for any business transaction involving an individual and its personal information.
018	5.3.6	Personal information shall not be used or disclosed by the seller (or regulator) for purposes other than for those it was originally collected as part of the business transaction, except with the informed consent of the individual, or as required by law. Secondary or derivative uses of personal information are not permitted.
019	5.3.6	Where the organization, having collected personal information for a specific purpose and goal of the execution of the business transaction, desires to use the relevant personal information for another purpose, it is necessary to obtain revised/new "informed consent" directly from the individual concerned.
020	5.3.6	Personal information shall be retained by the seller only for as long as is necessary for the fulfilment of those purposes as specified as part of the business transaction.
021	5.3.6	The seller shall identify to the buyer, especially where the buyer is an individual, any and all record retention requirements pertaining to the sets of recorded information forming part of the specified goal of a business transaction of applicable external constraints of jurisdictional domain(s) as a result of the actualization of the business transaction.
022	5.3.6	Where the seller offers a warranty, or extended warranty, as part of the business transaction, the seller shall inform the buyer, when the buyer is an individual, of the associated added records retention requirements for the personal information associated with the warranty (including the purchase by the individual of an extended warranty).
023	5.3.6	Where the buyer in a business transaction is an individual, the seller shall inform the individual of any and all records retention requirements of personal information which is recorded as the result of the actualization of the business transaction, including: 1) personal information which is required to actualize the business 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 business transaction.
024	5.3.6	Where the buyer in business transaction is an individual, the seller shall inform that individual of the applicable record retention conditions where these pertain to personal information.

Rule No.	Clause ID	Rule statement
(1)	(2)	(3)
025	5.3.6	Where a business transaction does not reach the actualization phase, any personal information collected by the organization in support of that business transaction shall be deleted by the organization (unless the individual concerned explicitly consents to the prospective seller to the retention of such personal information for a defined period of time).
026	5.3.7	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 business transaction.
027	5.3.8	Personal information shall be protected by operational procedures 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.
028	5.3.9	An organization shall have and make readily available to any Person specific information about its policies and practices pertaining to the management and interchange of personal information under its control.
029	5.3.10	An individual has the right to know whether or not an organization has personal information under its control on or about that individual.
030	5.3.10	An organization, subject to privacy protection requirements, upon receiving a request from an individual shall inform that individual 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 business transactions of that organization.
031	5.3.10	Where an organization discovers that it has personal information on the individual who made the request, that individual shall be given full and complete access to any and all personal information which the organization maintains on that individual (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).
032	5.3.10	Where an organization has and maintains personal information on the individual making the request for access to his/her personal information and such personal information does exist, the organization shall provide access to the personal information in a manner which is convenient to that individual.
033	5.3.11	An individual shall be able to challenge the accuracy and completeness of his or her personal information held by an organization with respect to a business transaction (and/or part of a general client file) and have it amended or deleted as appropriate.
034	5.3.11	An individual shall be able to challenge an organization concerning its compliance with the above privacy protection principles 1 through 10, 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).
035	5.4	An organization shall have in place policies and procedures in order to identify and tag (or label) all sets of recorded information (SRIs) which contain personal information and do so at the appropriate level of granularity to facilitate compliance with specific privacy protection requirements.
036	5.4	For a field or data element comprising the recorded information pertaining to a business transaction, for personal information the following requirements apply from a data interchange perspective, the need to ensure the provision of a tag(s) to note that 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.