International Standard

ISO/IEC 15944-17

First edition
2024-04

Information technology — Business operational view —

Part 17: Fundamental principles and rules governing Privacy-by-Design (PbD) requirements in an EDI and collaboration space context

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

Partie 17: Règles et principes fondamentaux régissant les exigences de protection de la vie privée par conception (PbD) dans un contexte d'EDI et d'espace de collaboration

Reference number
ISO/IEC 15944-17:2024(en)

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

Published in Switzerland

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **2**

4 Abbreviated terms **18**

5 Fundamental privacy protection principles **19**
5.1 Overview 19
5.2 Primary sources of privacy protection principles 20
5.3 Exceptions to the application of the privacy protection principles 20
5.4 Key eleven (11) privacy protection principles 20
5.5 Link to "consumer protection" and "individual accessibility" requirements 21
5.6 Requirements for tagging (or labelling) sets of personal information (SPIs) in support of privacy protection requirements (PPR) 22
5.7 Requirements for making all personal information (PI) available to the buyer where the buyer is an individual 22

6 Fundamental principles and rules governing Privacy by Design (PbD) requirements **22**
6.1 Overview 22
6.2 Fundamental principles of Privacy by Design 23
6.2.1 Privacy by Design Principle 1: Proactive not reactive; preventative not remedial 23
6.2.2 Privacy by Design Principle 2: Privacy as the Default Setting 23
6.2.3 Privacy by Design Principle 3: Privacy Embedded into Design 24
6.2.4 Privacy by Design Principle 4: Full Functionality — Positive-Sum, not Zero-Sum 25
6.2.5 Privacy by Design Principle 5: End-to-End Safeguards — Full Information Management Life Cycle (ILCM) Protection 25
6.2.6 Privacy by Design Principle 6: Visibility and Transparency — Keep it Open 26
6.2.7 Privacy by Design Principle 7: Respect for User Privacy — Keep it User-Centric 26
6.3 Exceptions to the application of any of the Privacy by Design principles 27
6.4 Mapping the eleven (11) Privacy Protection Principles (PPP) to the seven (7) Privacy by Design principles 27

7 Collaboration space and privacy protection **27**
7.1 Overview 27
7.2 Collaboration space: Role of consumer (as individual), vendor and regulator 28

8 Ensuring that personal information is 'under the control of' the organization throughout its ILCM **30**
8.1 Overview 30
8.2 Rules governing the specification of ILCM aspects of personal information 31
8.3 Implementing "under the control of" and accountability 31

9 Conformance statement **32**
9.1 Overview 32
9.2 Conformance to the ISO/IEC 14662 Open-edi Reference Model and the multipart ISO/IEC 15944 eBusiness standard 33
9.3 Conformance to ISO/IEC 15944-17 33
9.4 Conformance by agents and third parties to ISO/IEC 15944-17 33

Annex A (normative) **Consolidated controlled vocabulary definitions and associated terms, as human interface equivalents (HIEs), with cultural adaptability: English and French language equivalency in an IT standardization context** **34**

Annex B (normative) **Consolidated set of rules in existing Parts of ISO/IEC 15944 of particular relevance to PbD as external constraints on business transactions which apply to personal information (PI) in an EDI and collaboration space context** **37**

Annex C (informative) **Mapping ISO/IEC 15944-8 Privacy Protection Principles (PPP) to the Privacy by Design principles** **54**
Annex D (informative) **Exclusions to the scope of ISO/IEC 15944-17** **58**
Annex E (informative) **Fair Information Principles / Fair Information Practices** **60**
Annex F (informative) **Aspects currently not addressed** **61**
Bibliography **62**

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC have not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

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

This document is intended to be used in conjunction with ISO/IEC 14662, ISO/IEC 15944-1, ISO/IEC 15944-4, ISO/IEC 15944-5, ISO/IEC 15944-8 and ISO/IEC 15944-12.

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

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 and www.iec.ch/national-committees.

Introduction

0.1 Purpose and overview

The ISO/IEC 14662 and the ISO/IEC 15944 Business Operational View (BOV) series of standards focus on electronic data interchange (EDI) and “collaboration space” among Persons. Modelling business transactions using scenarios and scenario components includes specifying the applicable constraints on the data using explicitly stated rules. The ISO/IEC 14662 Open-edi Reference Model identifies two basic classes of constraints, "internal constraints" and "external constraints".

Jurisdictional domains are the primary source of external constraints on business transactions. Privacy protection is addressed as a common set of external constraint requirements coming from jurisdictional domains. Jurisdictional domains, such as UN member states and/or their administrative sub-divisions (see further 5.2 on sources of requirements), 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 used for the recording of personal information and/or its communication to other Persons.

The overall purpose of the PbD[2] approach is two folds: (1) to ensure that privacy protection requirements (as stated in applicable legal and/or regulatory requirements) are identified as early as possible in the business operational process; (2) are specified in a systematic and rule-based manner for those developing any IT systems within their organization.

The PbD approach has always been supported and embedded in ISO/IEC 15944 development work. The need for the multipart ISO/IEC series of standards to comply with and support privacy protection requirements was already incorporated in the1st edition of ISO/IEC 15944-1. The development of the multipart series of ISO/IEC 15944 eBusiness standards and relevant parts of the multipart ISO/IEC standard that focus on privacy protection requirements fully supports the seven (7) foundational principles of the PbD approach.[2] In particular, it provides the detailed rules, definitions and related guidelines necessary 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 for any personal information interchanged via EDI among parities to a particular business transaction.

This document highlights the requirements of ISO/IEC 14662 and ISO/IEC 15944 that focus on addressing commonly definable aspects of external constraints that relate to Privacy by Design in a privacy protection requirements (PPR) context when the source is a jurisdictional domain.[1)] 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.

This document also extends the requirements of ISO/IEC 14662 and ISO/IEC 15944 where relevant and describes the added business semantic descriptive techniques needed to support PbD aspects beyond privacy protection requirements (PPR) when modelling business transactions. PbD aspects are central to ensuring that PPR are embedded early on in the design, passed on and supported throughout the lifecycle of the personal information, among all the parties to a business transaction using EDI.

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

0.2.1 ISO/IEC 14662 "Open-edi Reference Model"[2)]

ISO/IEC 14662 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

1) See further sublause 0.2 below which identifies and summarizes the relevance of ISO/IEC 14662 and specific parts of the multipart ISO/IEC 15944 standard to this document.

2) The ISO/IEC 14462 *Open-edi Reference Model* serves as the basis of the 2000 Memorandum of Understanding (MOU) among ISO, IEC, ITU and the UN/ECE concerning [harmonization of standardization in the field of electronic business. See https://www.itu.int//ITU-T/e-business/files/mou.pdf

related views of the business transaction. 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.

The delivery of Privacy by Design and 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 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. This is 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.

The first is the Business Operational View (BOV). The second is the Functional Service View (FSV). ISO/IEC 14662:2010, Figure 1 illustrates the realm to which PbD aligns with the Open-edi environment.

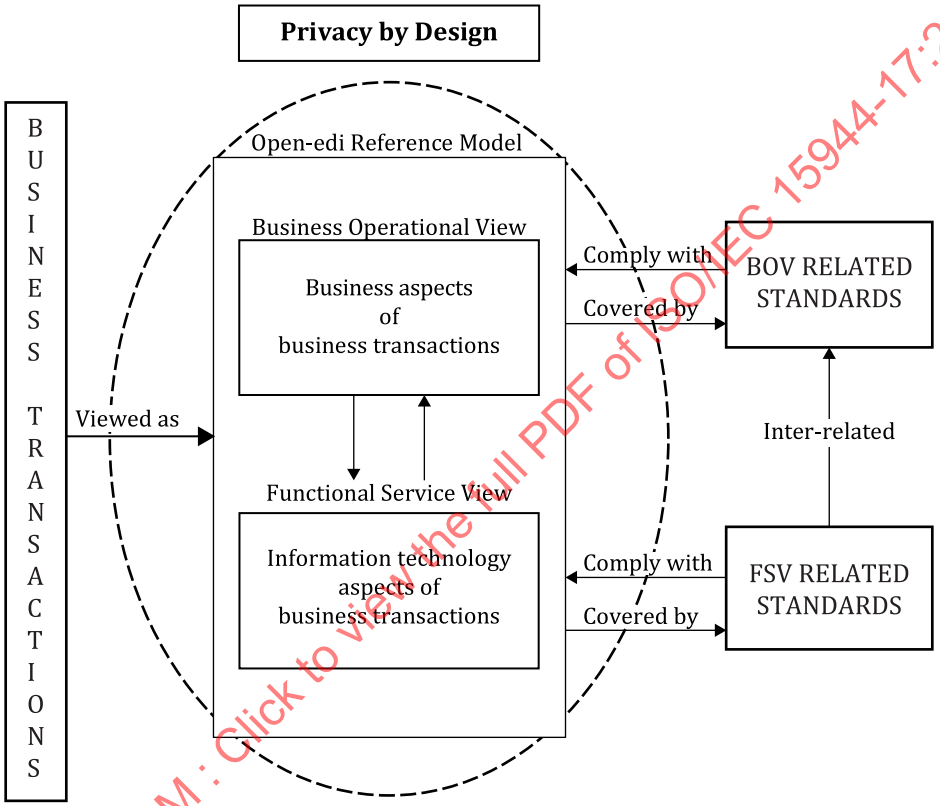

Figure 1 — Privacy by Design and Open-edi reference model environment

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 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, accessibility and human rights (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). 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 shows an integrated view of these business operational requirements. Since the focus of this document on Open-edi and Privacy by Design is that of external constraints for which jurisdictional domains are the primary source, these primary sources have been shaded (see 5.2 for sources of requirements).

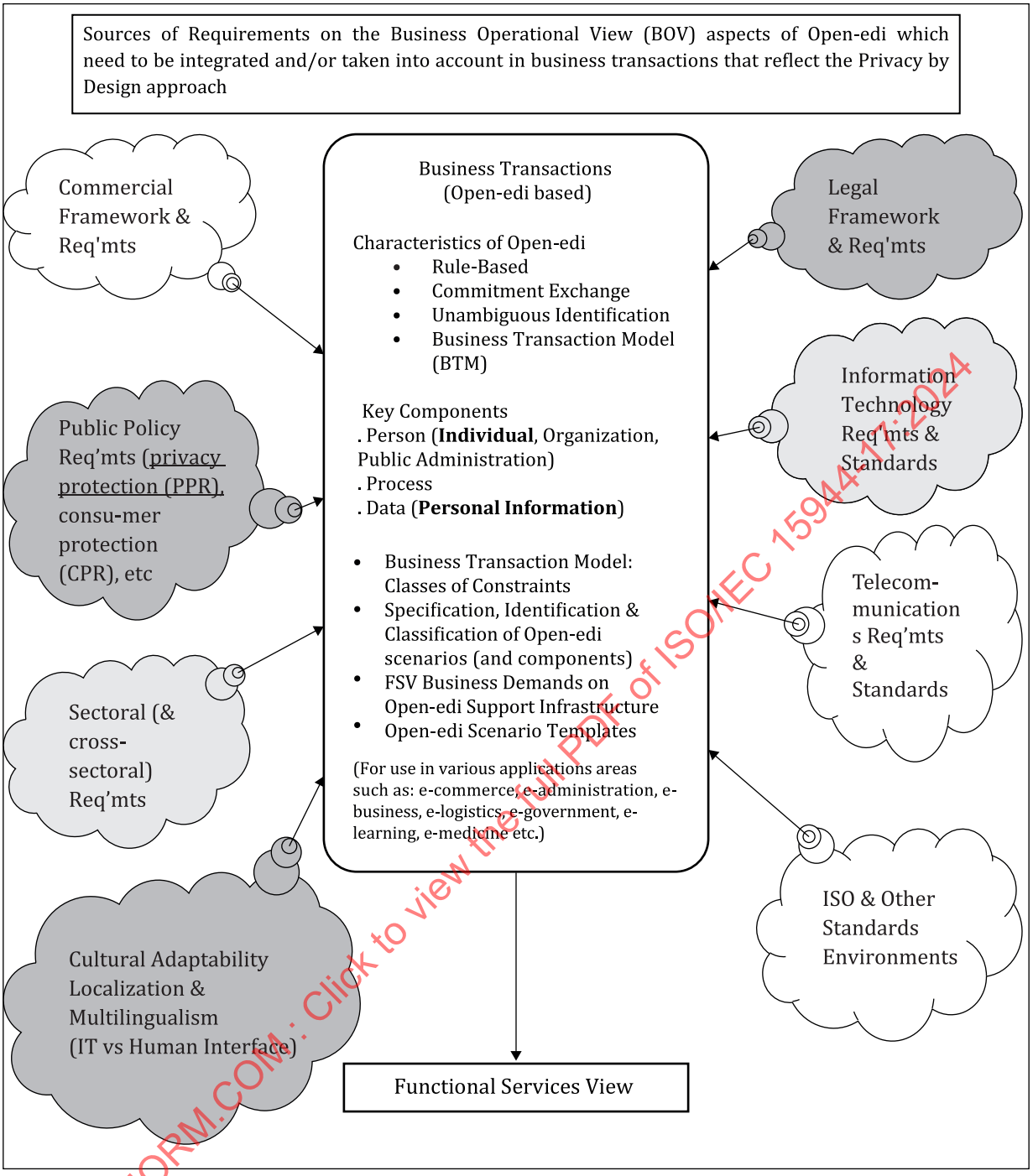

Figure 2 — Integrated view of business operational requirements with a focus on external constraints relevant to Privacy by Design

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[3)].

0.2.3 Links to ISO/IEC 15944-5, ISO/IEC 15944-8, ISO/IEC 15944-4 and ISO/IEC 15944-12

3) The text in this section is based on existing text in Section "0.3" in ISO/IEC 15944-1 and ISO/IEC 14662 (3rd edition). ISO/IEC 15944-7 "… eBusiness vocabulary" standard

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 identifies 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 uses ISO/IEC 15944-8 as the basis for establishing the fundamental privacy protection principles and rules that carry over to Privacy by Design. (Refer to Annex C.)

ISO/IEC 15944-4 helps to define the context in which PPP and PbD rules apply which is to the collaboration space. ISO/IEC 15944-4 provides the independent and the trading partner perspectives in the Open EDI ontology. In ISO/IEC 15944-1:2011, 6.1.3, Rule 1 states: *"Business transactions require both information exchange and commitment exchange."* REA firmly agrees with and helps give definition to this assertion. Reciprocal commitments are exchanged in REA via economic contracts that govern exchanges, while information exchange is tracked via business events that govern the state transitions of business transaction entities that represent various economic phenomena. (See further 7.2 for REA and collaboration space). It is the requirement for information exchange and more specifically, information exchange with an individual within a business transaction that will trigger privacy protection rules in an Open EDI environment.

ISO/IEC 15944-12 is based on both ISO/IEC 15944-5 and ISO/IEC 15944-8 and integrates applicable concepts and definitions, principles, rules, etc., found in both (as well as applicable elements of the Open-edi reference model and other parts of the ISO/IEC 15944 series). The focus is on information life cycle management (ILCM) aspects at a more granular level, i.e. that are required to be able to support implementation of the same. The focus 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. It describes the added business semantic descriptive techniques needed to support information life cycle management_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. ILCM is an important aspect of privacy protection and PbD.

0.3 Importance and role of terms and definitions[4)]

The ISO/IEC 15944 series sets out the processes for achieving a common understanding of the BOV from commercial, legal, ICT, public policy and cross-sectoral perspectives. It is 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 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 Chinese, French, and Russian.

0.4 Basic rules and guidelines

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

4) All the terms and definitions of the current editions of the ISO/IEC 14662 *Open-edi Reference Model* and the multipart ISO/IEC 15944 eBusiness standard have been consolidated in ISO/IEC 15944-7. A primary reason for having "Terms and definitions" in a standard is because one cannot assume that a common understanding exists, worldwide, for a specific concept. And even if one assumes that such an understanding exists, then having such a common definition in Clause 3 serves to formally and explicitly affirm (re-affirm) such a common understanding, i.e. ensure that all parties concerned share this common understanding as stated through the text of the definitions in Clause 3.

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 for which there is mutual agreement. 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.

0.5 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";

— 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.

0.6 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.

0.7 Use of "jurisdictional domain" in the context of privacy protection requirements and Privacy by Design

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.

0.8 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 can only apply to some proportion of the specific role players in a business transaction (including their personae) and not others.

0.9 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 an 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 PbD the concept and definition of SPI applies:

set of personal information (SPI)

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

This document focuses on PbD in support of PPR and as such "set of personal information (SPI)" is used throughout this document.

0.10 Aspects currently not addressed

The first edition of this document focuses on the essential and basic PbD aspects in an EDI and collaboration space context. Other aspects identified in the development of this document remain to be addressed. For detailed information, see Annex F.

0.11 IT-systems environment neutrality

This document, like all the other parts of ISO/IEC 15944, does not assume or 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.

0.12 Organization and description of this document

The focus of this document is on any kind of recorded personal information concerning individuals as buyers in a business transaction or whose personal information is used in a business transaction or any type of commitment exchange. (Refer to the exclusion of Publicly Available Personal Information (PAPI) in Annex D).

This document applies to any organization which receives, creates, process, maintains, communicates, etc. personal information (PI) of a consumer 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 organizations 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 design management 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.

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 context of PbD requirements.

The purpose and focus of Clause 6 is to apply the seven PbD requirements in Open-edi business transaction context using the ISO/IEC 15944 rule-based approach as they apply to any organization (or public administration) in their interaction with any individual (outside of their organization) in the role of that individual as a buyer, i.e. consumer, in its interaction with the organization.

The importance of the concept of "collaboration space" introduced in ISO/IEC 15944-4 is carried forward and adapted in the privacy protection context in Clause 7, as the "privacy collaboration space (PCS)".

Clause 8 summarizes the Information Lifecycle Management (ILCM) aspects of PbD as part of privacy protection requirements when modelling business transactions using the external constraints of jurisdictional domains defined in detail in ISO/IEC 15944-12:2020.

Clause 9 provided the conformance requirements for this document.

Annex A provides the HIEs for all the terms and definitions newly defined in this document in addition to other parts of ISO/IEC 15944.

Annex B provides a consolidated set of rules defined in ISO/IEC 15944 relevant to this document.

Annex C provides the mapping of Privacy Protection Principles (PPP) to the Privacy by Design principles.

Annex D is a further description to the scope to clarify the exclusions that this document is not specifying.

Annex E introduces the concept of Fair Information Principles/Fair Information Practices in more detail.

Annex F provides additional information to the scope, stating those aspects that are yet addressed by the content of this document.

Information technology — Business operational view —

Part 17: Fundamental principles and rules governing Privacy-by-Design (PbD) requirements in an EDI and collaboration space context

1 Scope

This document:

a) focuses on PbD aspects of privacy protection requirements as external constraints on any type of Person, (e.g. organization or public administration) involved in any kind of business transaction among such Persons which involves the electronic data interchange (EDI) of any personal information;

b) establishes a fundamental set of privacy principles known as Privacy by Design and assumptions based on primary sources;

c) integrates existing normative elements in support of PbD as are already identified in ISO/IEC 14662 and ISO/IEC 15944-1, ISO/IEC 15944-5, ISO/IEC 15944-8, ISO 15944-12;

d) provides overarching operational 'best practice' statements for associated (and not necessarily automated) processes, procedures, practices and governance requirements that need to act in support of implementing and enforcing technical mechanisms that support PbD in Open-edi transaction and collaboration space environments;

e) focuses on PbD related aspects of the life cycle management of and accountability for the 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.

This document focuses on the BOV aspects of a business transaction and does not concern itself with the technical mechanisms needed to implement the FSV aspects of the business requirements of the FSV including the specification of requirements of an FSV nature which include security techniques and services, communication protocols, etc.). The FSV includes any existing standard (or standards development of an FSV nature), which has been ratified by existing ISO, IEC, UN/ECE and/or ITU standards.

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

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 15944-1:2011, *Information technology — Business operational view — Part 1: Operational aspects of open-edi for implementation*

ISO/IEC 15944-4:2015, *Information technology — Business operational view — Part 4: Business transaction scenarios — Accounting and economic ontology*

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

ISO/IEC 15944-7:2009, *Information technology — Business Operational View — Part 7: eBusiness vocabulary*

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

ISO/IEC 15944-12:2020, *Information technology — Business operational view — Part 12: Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information (PI)*

3 Terms and definitions

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

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

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

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

3.1
agent
Person (3.41) acting for another *Person* in a clearly specified capacity in the context of a *business transaction* (3.4)

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 15944-1:2011, 3.1]

3.2
business
series of *processes* (3.51), each having a clearly understood purpose, involving more than one *Person* (3.41), realized through the exchange of *recorded information* (3.57) and directed towards some mutually agreed upon goal, extending over a period of time

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

3.3
Business Operational View
BOV
perspective of *business transactions* (3.4) limited to those aspects regarding the making of *business* (3.2) decisions and *commitments* (3.9) among *Persons* (3.41), which are needed for the description of a *business transaction*

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

3.4
business transaction
predefined set of activities and/or *processes* of *Persons* (3.41) which is initiated by a *Person* to accomplish an explicitly shared *business* (3.2) 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]

3.5
business transaction identifier
BTI
identifier assigned by a *seller* (3.63) or a *regulator* (3.58) to an instantiated *business transaction* (3.4) among the *Persons* (3.41) 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) can 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]

3.6
buyer
Person (3.41) 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 15944-1:2011, 3.8]

3.7
coded domain
domain for which: (1) the boundaries are defined and explicitly stated as a rulebase of a coded domain Source Authority; and, (2) each *entity* (3.19) which qualifies as a member of that domain is identified through the assignment of a unique *ID code* (3.24) in accordance with the applicable Registration Schema of that *Source Authority* (3.66)

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 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: 3 A coded domain is a data set for which the content values of the data element 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; and/or, (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 must 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 must 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]

3.8
collaboration space
business (3.2) 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]

3.9
commitment
making or accepting of a right, obligation, liability or responsibility by a *Person* (3.41) that is capable of enforcement in the *jurisdictional domain* (3.34) in which the *commitment* (3.9) is made

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

3.10
constraint
rule (3.61), explicitly stated, that prescribes, limits, governs or specifies any aspect of a *business transaction* (3.4)

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 15944-1:2011, 3.11]

3.11
consumer
buyer (3.6) who is an *individual* (3.27) to whom *consumer protection* (3.13) requirements are applied as a set of *external constraints* (3.21) on a *business transaction* (3.4)

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 can be peculiar to a specified jurisdictional domain.

[SOURCE: ISO/IEC 15944-1:2011, 3.12]

3.12
consumer information profile
CIP
any one or more, *personal information profiles (PIPs)* (3.44) and any related *personal information* (3.42) on or about an identifiable *individual* (3.27) to which *consumer protection* (3.13) requirements apply, i.e., in addition to applicable *privacy protection* (3.48) requirements

[SOURCE: ISO/IEC 15944-12:2020, 3.25]

3.13
consumer protection
set of *external constraints* (3.21) of a *jurisdictional domain* (3.34) as rights of a *consumer* (3.11) and thus as obligations (and possible liabilities) of a *vendor* (3.71) in a *business transaction* (3.4) which apply to the good, service and/or right forming the object of the *business transaction* including associated information management and interchange requirements including applicable *set(s) of recorded information (SRIs)* (3.65)

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 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 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]

3.14
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]

3.15
data element
unit of *data* (3.14) for which the definition, *identification* (3.25), representation and permissible values are specified by means of a set of attributes

[SOURCE: ISO/IEC 15944-1:2011, 3.15]

3.16
Decision Making Application
DMA
model of that part of an Open-edi system that makes decisions corresponding to the *role(s)* (3.60) that the Open-edi Party plays as well as the originating, receiving and managing *data* (3.14) values contained in the instantiated *Information Bundles* (3.29) which is not required to be visible to the other Open-edi Parties (OeP)

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

3.17
eBusiness
business transaction (3.4), involving the making of *commitments* (3.9), in a defined *collaboration space* (3.8), among *Persons* (3.41) using their *IT Systems* (3.32), according to *Open-edi standards* (3.37)

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 15944-7:2015, 3.06]

3.18
Electronic Data Interchange
EDI
automated exchange of any predefined and structured *data* (3.14) for *business* (3.2) purposes among information systems of two or more *Persons* (3.41)

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

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

3.19
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]

3.20
expungement
process of ensuring complete elimination, wiping out, destroying, or obliteration of any *recorded information* (3.57) (or *sets of recorded information (SRIs))* (3.65), 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

[SOURCE: ISO/IEC 15944-12:2020, 3.44]

3.21
external constraint
constraint (3.10) which takes precedence over *internal constraints* (3.36) in a *business transaction* (3.4), 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, (e.g., 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 can issue a prescription for a controlled drug.

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

EXAMPLE 3 Hazardous wastes can 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 can 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 15944-1:2011, 3.23]

3.22
Functional Service View
FSV
perspective of *business transactions* (3.4) limited to those information technology interoperability aspects of *IT Systems* (3.32) needed to support the execution of *Open-edi transactions*

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

3.23
Human Interface Equivalent
HIE
representation of the *unambiguous* (3.69) and IT-enabled semantics of an IT interface equivalent (in a *business transaction* (3.4)), often the *ID code* of a *coded domain* (or a composite identifier, in a formalized manner suitable for communication to and understanding by humans

Note 1 to entry: Human interface equivalents can be linguistic or non-linguistic in nature but their semantics remain the same although their representations can 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, (e.g., in addition to written text those of an audio, symbol (and icon) nature, glyphs, image, etc.).

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

3.24
ID code
identifier assigned by the *coded domain* (3.7) Source Authority (cdSA) to a member of a *coded domain* ID

Note 1 to entry: ID codes must 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; (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 must 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 must 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 modeling notation, an ID code is viewed as an instance of an object class.

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

3.25
identification
rule-based *process*, explicitly stated, involving the use of one or more attributes, i.e., *data element(s)* (3.15), whose value (or combination of values) are used to identify uniquely the occurrence or existence of a specified *entity* (3.19)

[SOURCE: ISO/IEC 15944-1:2011, 3.26]

3.26
identifier (in a business transaction)
unambiguous (3.69), unique and a linguistically neutral value, resulting from the application of a rule-based *identification* (3.25) *process* (3.51)

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 19135-1:2015, 4.1.5}

[SOURCE: ISO/IEC 15944-1:2011, 3.27]

3.27
individual
Person (3.41) who is a human being, i.e., a natural person, who acts as a distinct indivisible *entity* (3.19) or is considered as such

[SOURCE: ISO/IEC 15944-1:2011, 3.28]

3.28
individual accessibility
set of *external constraints* (3.21) of a *jurisdictional domain* (3.34) as rights of an *individual* (3.27) with disabilities to be able to use *IT Systems* (3.32) at the human, i.e., user, interface and the concomitant obligation of a *seller* (3.63) 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]

3.29
Information Bundle
IB
formal description of the semantics of the *recorded information* (3.57) to be exchanged by Open-edi parties playing *roles* (3.60) in an Open-edi scenario

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

3.30
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* (3.57), 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]

3.31
information life cycle management
ILCM
series of actions and *rules* (3.61) governing the management and its *Electronic Data Interchange (EDI)* (3.18) of *set(s) of recorded information (SRIs)* (3.65) *under the control of* (3.70) a *Person* (3.41) from its creation to final disposition, including *expungement* (3.20), in compliance with applicable *information law* (3.30) requirements

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

[SOURCE: ISO/IEC 15944-12:2020, 3.58]

3.32
Information Technology System
IT System
set of one or more computers, associated software, peripherals, terminals, human operations, physical *processes* (3.51), information transfer means, that form an autonomous whole, capable of performing information processing and/or information transfer

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

3.33
internal constraint
constraint (3.10) which forms part of the *commitment(s)* (3.9) mutually agreed to among the parties to a *business transaction* (3.4)

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 15944-1:2011, 3.33]

3.34
jurisdictional domain
jurisdiction, recognized in law as a distinct legal and/or regulatory framework, which is a source of *external constraints* (3.21) on *Persons* (3.41), their behaviour and the making of *commitments* (3.9) among *Persons* including any aspect of a *business transaction* (3.4)

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) can 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 The European Union (EU), NAFTA, WTO, WCO, ICAO, WHO, Red Cross, the ISO, the IEC, the ITU, etc.

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

Note 4 to entry: A jurisdictional domain can 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]

3.35
medium
physical material which serves as a functional unit, in or on which information or *data* (3.14) 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) form or format of recorded information; (b) 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 15944-1:2011, 3.34]

3.36
Open-edi
Electronic Data Interchange (3.18) *(EDI)* among multiple autonomous *Persons* (3.41) to accomplish an explicit shared *business* (3.2) goal according to *Open-edi standards* (3.37)

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

3.37
Open-edi standard
standard (3.67) that complies with the *Open-edi* (3.36) Reference Model

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

3.38
Open-edi transaction
business transaction (3.4) that is in compliance with an Open-edi scenario

[SOURCE: ISO/IEC 15944-1:2011, 3.43]

3.39
organization
unique framework of authority within which a *Person* (3.41) 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 15944-1:2011, 3.44]

3.40
organization Person
organization part which has the properties of a *Person* (3.41) and thus is able to make *commitments* (3.9) on behalf of that *organization* (3.39)

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 15944-1:2011, 3.46]

3.41
Person
entity (3.19), i.e., a natural or legal person, recognized by law as having legal rights and duties, able to make *commitment(s)* (3.9), 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]

3.42
personal information
PI
any information on or about an identifiable *individual* (3.27) 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]

3.43
personal information controller
PIC
organization Person (3.40) authorized and so formally designated by the *organization* (3.39) to ensure that *personal information* (3.42) remains (fully) *under the control of* (3.70) the *organization* and ensures its privacy protection transactional integrity (PPTI) in compliance with applicable *privacy protection* (3.48) requirements including in any use by the *organization* of *agents* (3.1) and/or *third parties* (3.68) in support of a *business transaction(s)* (3.4)

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" in case a seller decides 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 can 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 is possible 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.

[SOURCE: ISO/IEC 15944-12:2020, 3.91]

3.44
personal information profile
PIP
any collection of *personal information (PI)* (3.42) or aggregation of *sets of personal information (SPIs)* (3.64) including associated identifiers, linkages and/or associations, on or about an identifiable *individual* (3.27) being collected, retained, managed, used, etc., by any other *Person* (3.41) and in particular an *organization* (3.39) *or public administration* (3.54) and as such to which *privacy protection* (3.48) requirements apply including those of a *ILCM* (3.31) 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.

[SOURCE: ISO/IEC 15944-12:2020, 3.92]

3.45
Person identity
Pi
combination of *personal information* (3.42) and identifier used by a *Person* (3.41) in a *business transaction* (3.4)

[SOURCE: ISO/IEC 15944-12:2020, 3.93]

3.46
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]

3.47
privacy collaboration space
modelling or inclusion in an Open-edi scenario of a *collaboration space* (3.8) involving an *individual* (3.27) as the *buyer* (3.6) in a potential or actualized *business transaction* (3.4) where the *buyer* is an *individual* and therefore privacy protection requirements apply to *personal information* (3.42) of that *individual* provided in that *business transaction*

[SOURCE: ISO/IEC 15944-8:2012, 3.107]

3.48
privacy protection
set of *external constraints* (3.21) of a *jurisdictional domain* (3.34) pertaining to *recorded information* (3.57) on or about an identifiable *individual* (3.27), i.e., *personal information* (3.42), 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]

3.49
Privacy by Design
PbD
approach whose objective is to embed *privacy protection* (3.48) requirements for the *processing of personal information* (3.42) into the development and operation of *IT Systems* (3.32) and networks of an *organization* (3.39) as early as possible (proactively) and throughout the *information life cycle management (ILCM)* (3.31) of *personal information* with the goal of full compliance with applicable privacy protection requirements including reducing the risk of unauthorized collection, use, interchange, and/or disclosure of such *personal information*

3.50
privacy protection officer
PPO
organization Person (3.40) authorized by the *organization* (3.39) 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* (3.48) requirements for *information life cycle management* (3.31) not only within that *organization* but also with respect to any *Electronic Data Interchange* (3.18) of *personal information* on the *individual* (3.27) concerned with parties to the *business transaction* (3.4), including a *regulator* (3.58) where required, as well as any *agents* (3.1), *third parties* (3.68) involved in that *business transaction*

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

3.51
process
series of actions or events taking place in a defined manner leading to the accomplishment of an expected result

[SOURCE: ISO/IEC 15944-1:2011, 3.53]

3.52
processing of personal information
any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction

[SOURCE: ISO/IEC 15944-8:2012, 3.118]

3.53
pseudonym
use of a persona or other identifier by an *individual* (3.27) which is different from that used by the *individual* with the intention that it be not linkable to that *individual*

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

3.54
public administration
entity (3.19), i.e., a *Person* (3.41), which is an *organization* (3.39) and has the added attribute of being authorized to act on behalf of a *regulator* (3.58)

[SOURCE: ISO/IEC 15944-1:2011, 3.54]

3.55
public policy
category of *external constraints* (3.21) of a *jurisdictional domain* (3.34) specified in the form of a right of an *individual* (3.27) or a requirement of an *organization* (3.39) and/or *public administration* (3.54) with respect to an *individual* pertaining to any exchange of *commitments* (3.9) among the parties concerned involving a good, service and/or right including information management and interchange requirements

Note 1 to entry: Public policy requirements can apply to any one, all or combinations of the fundamental activities comprising a business transaction, i.e., planning, identification, negotiation, actualization and post-actualization.

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 can 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]

3.56
publicly available personal information
PAPI
personal information (3.42) about an *individual* (3.27) 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]

3.57
recorded information
information that is recorded on or in a *medium* (3.35) 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 15944-1:2011, 3.56]

3.58
regulator
Person (3.41) who has authority to prescribe *external constraints* (3.21) which serve as *principles* (3.46), policies or *rules* (3.61) governing or prescribing the behaviour of *Persons* involved in a *business transaction* (3.4) as well as the provisioning of goods, services, and/or rights interchanged

[SOURCE: ISO/IEC 15944-1:2011, 3.59]

3.59
retention period
length of time for which *data* (3.14) on a *data medium* (3.35) is to be preserved

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

3.60
role
specification which models an external intended behaviour (as allowed within a scenario) of an Open-edi Party

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

3.61
rule
statement governing conduct, procedure, conditions and relations

Note 1 to entry: Rules specify conditions that should be complied with. These can 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]

3.62
scenario
formal specification of a class of *business* (3.2) activities having the same *business* goal

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

3.63
seller
Person (3.41) who aims to hand over voluntarily or in response to a demand, a good, service and/or right to another *Person* (3.41) and in return receives an acceptable equivalent value, usually in money, for the good, service and/or right provided

[SOURCE: ISO/IEC 15944-1:2011, 3.62]

3.64
set of personal information
SPI
set of recorded information (SRI) (3.65) which is of the nature of, or contains, *personal information* (3.42)

[SOURCE: ISO/IEC 15944-12:2020, 3.127]

3.65
set of recorded information
SRI
recorded information (3.57) of a *Person* (3.41), which is *under the control of* (3.70) the same and which is treated as a unit in its information life cycle

Note 1 to entry: An 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: An 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: An 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]

3.66
Source Authority
SA
Person (3.41) recognized by other *Persons* as the authoritative source for a set of *constraints* (3.10)

Note 1 to entry: A Person as a Source Authority for internal constraints can be an individual, organization, or public administration.

Note 2 to entry: A Person as Source Authority for external constraints can 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]

3.67
standard
documented agreement containing technical specifications or other precise criteria to be used consistently as *rules* (3.61), guidelines, or definitions of characteristics, to ensure that materials, products, processes and services are fit for their purpose

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

[SOURCE: ISO/IEC 15944-1:2011, 3.64]

3.68
third party
Person (3.41) besides the two primarily concerned in a *business transaction* (3.4) who is *agent* (3.1) of neither and who fulfils a specified *role* (3.60) or function as mutually agreed to by the two primary *Persons* or as a result of *external constraints* (3.21)

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 15944-1:2011, 3.65]

3.69
unambiguous
level of certainty and explicitness required in the completeness of the semantics of the *recorded information* (3.57) interchanged appropriate to the goal of a *business transaction* (3.4)

[SOURCE: ISO/IEC 15944-1:2011, 3.66]

3.70
under the control of
set of requirements on an *organization* (3.39), especially those of *external constraint* (3.21) nature, i.e., *privacy protection* (3.48) and related *information law* (3.30) requirements, requiring full and complete *information life cycle management (ILCM)* (3.31) of *personal information* (3.42) as *set(s) of recorded information (SRIs)* (3.65) related to the agreed upon goal of the instantiated *business transaction* (3.4), 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* (3.20)), *Electronic Data Interchange (EDI)* (3.18), etc., and in particular that of any and all state changes in the *decision making application (DMAs)* (3.16) of the *organization* and any of its *agents* (3.1) and/or *third parties* (3.68) (as well as any other parties) to the *business transaction*

Note 1 to entry: The fact that a Person responsible for the control of an 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.

[SOURCE: ISO/IEC 15944-12:2020, 3.142]

3.71
vendor
seller (3.63) on whom *consumer protection* (3.13) requirements are applied as a set of *external constraints* (3.21) on a *business transaction* (3.4)

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 can be specific to a jurisdictional domain.

[SOURCE: ISO/IEC 15944-1:2011, 3.67]

4 Abbreviated terms

BOV	Business Operational View
BTI	Business Transaction Identifier
BTM	Business Transaction Model
CRPD	(UN) Convention on Rights of Persons with Disabilities
CIP	Consumer Information Profile
DMA	Decision Making Application
EDI	Electronic Data Interchange
FDT	Formal Description Technique
FIP	Fair Information Principles / Fair Information Practices
FSV	Functional Service View
GDPR	General Data Protection Directive
HIE	Human Interface Equivalent
IB	Information Bundle
ICT	Information communication technologies
IT System	Information technology system
ILCM	Information life cycle management
OeS	Open-edi scenario
PAPI	publicly available personal information
PbD	Privacy by Design
PCS	Privacy Collaboration Space
Pi	personal identity
PI	personal information
PIC	personal information controller
PIP	personal information profile
PPO	privacy protection officer
PPP	Privacy Protection Principles
PPR	privacy protection requirement
PPTI	privacy protection transactional integrity
RBT	regulatory business transaction
rii	recognized individual identity

rPi	recognized Person identity
REA	Resource, Events, Agents
SA	Source Authority
SC	Semantic Component
SPI	set of personal information
SRI	set of recorded information

5 Fundamental privacy protection principles

5.1 Overview

This Clause is based primarily on ISO/IEC 15944-8:2012 and, in particular, its Clause 5. The applicable rules are found in ISO/IEC 15944-8:2012, B.5. In addition, relevant rules of ISO/IEC 15944-1, ISO/IEC 15944-4, ISO/IEC 15944-5, and ISO/IEC 15944-12 are identified in Annex B.

ISO/IEC 15944-8:2012 is a BOV-related standard which addresses basic (or primitive) requirements of a privacy protection environment, as legal requirements represented through jurisdictional domains, on business transactions, and also integrates the requirements of the information technology and telecommunications environments. It contains a methodology and tool for specifying common classes of external constraints through the construct of "jurisdictional domains". It meets the requirements set in ISO/IEC 15944-1 and ISO/IEC 15944-2 through the use of explicitly stated rules, templates, and Formal Description Techniques (FDTs).

This document begins with ISO/IEC 15944-8 as the basis to establish the fundamental privacy protection principles rules that carry over to Privacy by Design. (Refer to Annex C.) In Clause 6, the importance of the “collaboration space” introduced in ISO/IEC 15944-4, is carried forward in a privacy protection context in ISO/IEC 15944-8 as “privacy collaboration space (PCS)”. The concept of PCS is extended to include those aspects of a Privacy by Design nature. It is important to note that privacy protection is a right of an “individual” only and not of an organization or public administration.

ISO/IEC 15944-12 is based on both ISO/IEC 15944-5 and ISO/IEC 15944-8 and integrates applicable concepts and definitions, principles, rules, etc. found in both (as well as applicable elements of the Open-edi reference model and other parts of the ISO/IEC 15944 series). The focus of ISO/IEC 15944-12 is on information life cycle management (ILCM) aspects at a more granular level, i.e. that are required to be able to support implementation of the same. Consequently, ILCM is an important aspect of privacy protection and PbD and the reference to this in Clause 8.

Rule 001:

The rules identified in Annex B, as taken from ISO/IEC 15944-1, ISO/IEC 15944-4, ISO/IEC 15944-5 and ISO/IEC 15944-12 shall be applied to the normative Clauses and Annexes of this document.

Rule 002:

The rules, guidelines and associated normative text as stated in ISO/IEC 15944-8:2012, 5.3 that identify the eleven (11) privacy protection principles (PPP) shall apply to this document.

The Open-EDI eleven (11) privacy protection principles are affirmed by the Privacy by Design framework. The PbD framework is a holistic approach to design privacy protection into technologies, business processes and systems prior to processing personal information.

In particular, three of the seven PbD principles expand upon PPP to reflect the pervasiveness of technology and growing digitization of data.

5.2 Primary sources of privacy protection principles

Figure 3 is adapted from ISO/IEC 15944-8:2012, Figure 3. It is repeated to provide an updated overview of the sources of requirements of the privacy protection principles as they also apply to this document. The EU "General Data Protection Directive" (GDPR) replaced the EU "Directive 95/46/EC of the European Parliament"[10] and refers to "data protection by design and by default" in its Article 25.

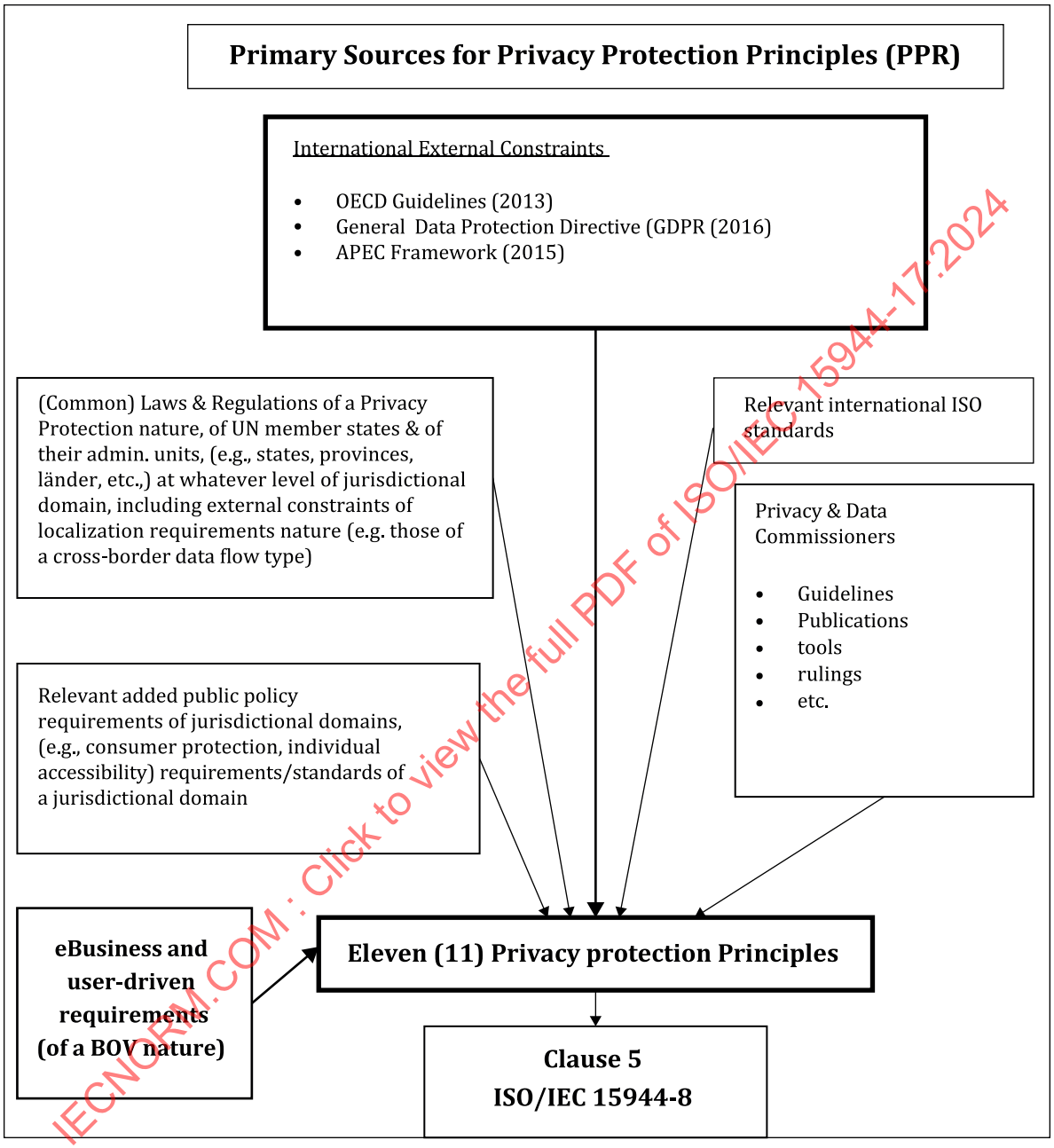

Figure 3 — Primary sources for privacy protection principles

5.3 Exceptions to the application of the privacy protection principles

The rules stated in ISO/IEC 15944-8:2012, 5.2, along with the interpretation specified in 5.2, shall apply.

5.4 Key eleven (11) privacy protection principles

Rule 003:

The rules stated in ISO/IEC 15944-8:2012, 5.3 that reference eleven (11) fundamental privacy protection principles, rules, guidelines and associated normative text apply to this document.

The principles 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

A summary of the complete set of rules (with guidelines where applicable) and associated normative text is provided for each PPP in the PbD context in Annex C, Table C.2.

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 an 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 to 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.

Finally, as with Privacy by Design, the privacy protection principles enumerated above represent a whole and should be interpreted and implemented as a whole and not piecemeal.

5.5 Link to "consumer protection" and "individual accessibility" requirements

This document, as with ISO/IEC 15944-5 and ISO/IEC 15944-8 (ISO/IEC 15944-8:2012, 6.3 Collaboration space: The role of buyer (as individual), seller and regulator), 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.

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[6];

   — REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 The General Data Protection Regulation (GDPR)[9]

   — APEC Privacy Framework. (2015)[7]

   — UN Convention on the Rights of Persons with Disabilities (CRPD) (2006+)[8].

3) There are other external constraints of a "public policy" nature which need to be taken into account in modelling business transactions. These include “individual accessibility”, human rights, etc. In ISO/IEC 15944-1:2011, 6.1.6, these form part of the category of *"External Constraints: Public Administration*" (as identified in ISO/IEC 15944-1:2011, Figure 8).

Rule 004:

The rules stated in ISO/IEC 15944-8:2012, 7.2.1 Privacy protection, 7.2.2, 7.2.3, 7.2.4, 7.2.5 apply to this document.

5.6 Requirements for tagging (or labelling) sets of personal information (SPIs) in support of privacy protection requirements (PPR)

Rule 005:

The rules stated in ISO/IEC 15944-8:2012, 5.4 apply to this document. The application of privacy protection requirements requires an organization to be able to identify and tag any and all personal information when it is created or recorded in its IT systems.

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

Rule 006:

The rules stated in ISO/IEC 15944-12:2020, 5.7 apply to this document. It is a best business practice as well as a contractual and consumer protection requirement for the seller to make the buyer, as in individual, aware of all personal information pertaining to that business transaction and to do so in a timely manner.

6 Fundamental principles and rules governing Privacy by Design (PbD) requirements

6.1 Overview

Privacy by Design not only embodies the universal principles of the Fair Information Practices[11] (See Annex E), but also provides a set of added necessary and complementary principles intended to reflect the pervasiveness of technology and growing digitization of data. These complementary principles are reflected in the first four Foundational Principles: i) Principle 1. Proactive not Reactive, Preventative not Remedial; ii) Principle 2. Privacy as the Default; iii) Principle 3. Privacy Embedded into Design; and iv) 4. Full Functionality – Positive-Sum, not Zero-Sum.

Privacy by Design principles can assure effective organizational privacy and security by:

a) serving as a framework for specific data management and interchange control objectives (see Clause 8) and best practices;

b) reducing harms and other “unintended” consequences associated with personal information;

c) strengthening internal accountability mechanisms;

d) demonstrating effectiveness and credibility of data management practices;

e) supporting regulatory and third-party oversight efforts;

f) earning the confidence and trust of clients, partners and the public;

g) promoting market-based innovation, creativity and competitiveness;

h) and ensuring that personal information remains under the control of the organization.

6.2 Fundamental principles of Privacy by Design

6.2.1 Privacy by Design Principle 1: Proactive not reactive; preventative not remedial

Much of the text in 6.2 is adapted in summary form and placed in an Open-edi and eBusiness transaction context from PbD publication sources[2].

The PbD approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after. This requires clear leadership priorities to set and enforce the highest privacy protection requirements at the beginning of any IT systems development involving the use of personal information.

Rule:007:

This clear commitment at the highest level within an organization also shall apply to any electronic data interchange (EDI) of personal information of individuals as in their role as a consumer in the provision of a good, service, and/or right by the organization.

Rule 008:

There shall be a clear commitment, at the highest levels within an organization, to set and enforce high standards of privacy protection – higher than the minimal standards set out by global laws and regulations which serve as external requirements on any personal information including any EDI of the same with the individual concerned as well as any agents or third parties with which the organization interchanges personal information of an individual.

Rule 009:

Commitment to privacy protection requirements shall be demonstrable and shared throughout the organization, with its user communities and other parties to the transaction (e.g. consumers, agents, third parties, etc.), in a culture of continuous improvement.

Rule 010:

There shall be established methods to: i) identify lack of, absence of or poorly designed privacy protection controls, ii) identify associated risks to privacy protection; iii) remediate the risks based on interest of the parties and the negative impacts before they occur in proactive, systematic, and innovative ways.

Guideline 010G1:

While risk management approach has it benefits, an organization should take a quality and integrity approach as a best practice as since such an approach will minimize risks.

6.2.2 Privacy by Design Principle 2: Privacy as the Default Setting

Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal information (PI) are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the IT system(s) of the organization, by default.

The PbD default settings of a PbD approach include the following:

— Purpose Specification;

— Collection Limitation;

— Data Minimization; and,

— Use, Retention and Disclosure Limitation.

The rules and guidelines supporting each of these PbD default setting are as follows.

Rule 011:

Purpose Specification: the purposes for which personal information is collected, used, retained and disclosed shall be communicated to the individual at or before the time the information is collected.

Guideline 011G1:

Specified purposes should be clear, limited and relevant to the goal of the business transaction between an organization and any individual (as in its role as a consumer).

Rule 012:

Collection Limitation: the collection of personal information shall be fair, lawful and limited to that which is necessary for the specified purpose as stated and agreed to in the business transaction between the organization and the individual as its (potential) consumer.

Rule 013:

Data Minimization: the collection of personal information should be kept to a strict minimum as required to meet the requirements of an instantiated business transaction between the organization and an individual as a (potential) consumer of the goods, services, and/or right being provided by the organization.

Guideline 013G1:

The design of IT systems (and associated data and software programs) should in their design, development and implementation differentiate between any recorded information which a) does not contain personal information, and b) that which does. This is important to support privacy protection requirements which exclude any possible identifiability, observability and linkability of personal information pertaining to an individual.

Rule 014:

Use, Retention, and Disclosure Limitation: – the use, retention, and disclosure of personal information shall be limited to the relevant purposes identified to the individual, for which he or she has consented, except where otherwise required by law.

Rule 015:

Personal information shall be retained only as long as necessary to fulfill the stated purpose(s), and then destroyed, i.e., expunged in accordance with the rules stated in ISO/IEC 15944-12 pertaining to information life cycle management.

6.2.3 Privacy by Design Principle 3: Privacy Embedded into Design

PbD is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality. It means verifiable commitment to these priorities in all design and operational processes. A systemic program or methodology should be in place to ensure that privacy commitments are thoroughly integrated into the technology, process or architecture in question.

Rule 016:

A systematic, principle-based approach to embedding privacy protection requirements shall be adopted by any organization which in its operations involves personal information.

Guideline 16G01:

An organization should apply fair information practices (FIP) with equal rigour at every step in the design and operation of any business transaction of that organization (e.g., through its specification of a (reusable/repeatable) scenario(s) governing such specified business transaction.

Rule 017:

Detailed risk and impact assessments shall be carried out and published, i.e., one that clearly documents the privacy protection risks and all measures taken to mitigate those risks, including consideration of alternatives and selection of metrics.

Rule 018:

The requirements of privacy protection impacts on the resulting IT systems, their operation, or information architecture, and their uses shall be demonstrably minimized and not easily degraded through use, misconfiguration or error.

6.2.4 Privacy by Design Principle 4: Full Functionality — Positive-Sum, not Zero-Sum

PbD accommodates and supports all legitimate interests and objectives in a positive-sum "win-win" manner, not where unnecessary trade-offs are made[3][4]. PbD avoids the pretence of false dichotomies, such as privacy versus security, demonstrating that it is possible to have both. It includes demonstrating practical, measurable and proven results that reflect the presence of multiple objectives. All legitimate non-privacy objectives and functionalities should be accommodated (taking an innovative approach).

Rule 019:

An organization shall ensure that when it embeds privacy protection requirements into any of its information life cycle management (ICLM) processes, and its supporting IT Systems, that this shall be done in such a way that full functionality of support for privacy protection requirements is not impaired, and that all privacy protection requirements are optimized in the design and operation of any business transaction, (e.g., through its specification of re-useable scenarios governing such specified business transactions).

Rule 020:

All interests and objectives shall be clearly documented, desired functions articulated, metrics agreed upon and applied, and trade-offs rejected as often being unnecessary, in favour of finding a solution that enables multi-functionality.

Privacy protection is often positioned as having to compete with other legitimate human values, design objectives, and technical capabilities in a given domain. Privacy by Design rejects taking such an approach - it embraces legitimate non-privacy objectives and accommodates them all in an innovative positive-sum manner.

Rule 021:

An organization shall ensure that all times throughout the life cycle of personal information that such personal information remains under its control including in the organization's use of agents or third parties, and especially personal information that forms part of EDI interactions in support of any form of business transaction.

6.2.5 Privacy by Design Principle 5: End-to-End Safeguards — Full Information Management Life Cycle (ILCM) Protection

Privacy by Design, having been embedded into the IT system prior to the first element of personal information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy protection, from start to finish. This ensures that all data are securely retained, and then destroyed at the end of the ILCM process, in a timely fashion. Thus, Privacy by Design ensures cradle-to-grave, information lifecycle management of personal information, end-to-end.

Rule 022:

Safeguarding: Organizations shall assume responsibility for the safeguarding of personal information (commensurate with its degree of sensitivity) throughout its entire lifecycle,).

Rule 023:

Organizations shall assure the confidentiality, integrity and availability of personal information throughout its lifecycle and include, inter alia, methods of secure destruction, appropriate encryption, and strong access control and logging methods.

6.2.6 Privacy by Design Principle 6: Visibility and Transparency — Keep it Open

PbD seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, and applicable legal requirements, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike.

Rule 024:

Accountability: Collection of personal information entails a duty of care for its protection. Responsibility for all privacy protection related policies and procedures shall be documented by the organization and communicated as appropriate and assigned to a specified officer within the organization.

Rule 025:

When transferring personal information to third parties, equivalent privacy protection through contractual or other means shall be secured, documented and transparent.

Rule 026:

Openness: Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information shall be made readily available to the individual to whom the personal information pertains.

Rule 027:

Compliance: Complaint and redress mechanisms shall be established, and information communicated about them to the individual to whom the personal information pertains, including how to access the next level of appeal.

Guideline 027G1:

Necessary steps to monitor, evaluate, and verify compliance with privacy protection policies and procedures should be taken.

6.2.7 Privacy by Design Principle 7: Respect for User Privacy — Keep it User-Centric

Above all, PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy protection defaults, appropriate notice, and empowering user-friendly options. Respect for User Privacy extends to the need for human-machine interfaces to be human-centred, user-centric and person-friendly so that informed privacy decisions can be reliably exercised. Similarly, business operations and physical architectures should also demonstrate the same degree of consideration for the individual to whom the personal information pertains.

Rule 028:

Consent: The individual's free and specific consent is required for the collection, use or disclosure of any and all personal information, except where otherwise permitted by law. The greater the sensitivity of the personal data, the clearer and more specific the quality of the consent required. An individual shall be able to withdraw consent at any time.

Rule 029:

Accuracy: personal information shall be as accurate, complete, and up-to-date as is necessary to fulfil the specified purposes.

Rule 030:

Access: Individuals shall be provided access to their personal information and informed of its uses and disclosures. Individuals shall be able to challenge the accuracy and completeness of their personal information and have it amended as appropriate.

Rule 031:

Compliance: Organizations shall establish complaint and redress mechanisms, and communicate information about them to the public, including how to access the next level of appeal.

6.3 Exceptions to the application of any of the Privacy by Design principles

Privacy protection requirements of jurisdictional domains can contain exceptions (derogations) to the application of external constraints of this nature. The most common exceptions are those relating to national sovereignty and security, law enforcement.

Although PbD is intended as a holistic framework, there can be exceptions to the application of each of the (7) Foundational Principles. For example, if the IT system does not involve the direct interaction with an individual, then Principle 6 concerning transparency to the individual is not applicable.

Rule 032:

Where exceptions to the application of the PbD framework exist, they shall be:

1) **limited, proportional and effective**[5] **to meeting the objectives to which these exceptions relate;**

2) **made known to the public; or**

3) **in accordance with law of the applicable jurisdictional domain(s).**

6.4 Mapping the eleven (11) Privacy Protection Principles (PPP) to the seven (7) Privacy by Design principles

The development of the PPP has a long history and is focused on identifying and integrating the primary sources of requirements (see 5.2 and Figure 3). The development of the PbD approach and its seven (7) principles is driven from an implementation perspective of the PPP.

Rule 033: Users of this document shall be guided on the relationship between the eleven PPP principles and seven PbD principles as found in Annex C.

It is therefore important to "map" the relations and interactions between these two sets of principles. This has been done and the results are presented in Annex C. At the same time, 5.4 simply lists the eleven PPP. Annex C provides summary information on each PPP.

7 Collaboration space and privacy protection

7.1 Overview

The focus of these Open-edi and eBusiness standards is modelling the collaboration space among the primary parties to a business transaction. The business transaction requires at the least, the roles of a buyer and a seller, based on internal constraints only. Depending on the nature of the good, service and/or right (or

5) Also refer to the Oakes Test arising out of the Supreme Court of Canada - a test that is used every time a *Charter* violation is found. Section 1 of the *Charter* is often referred to as the "reasonable limits clause" because it is the section that can be used to justify a limitation on a person's *Charter* rights. *Charter* rights are not absolute and can be infringed if the Courts determine that the infringement is reasonably justified[12].

combination of the same) one or more sets of "external constraints" can apply. These are modelled through the introduction of the role of a "regulator".

The collaboration space was first established along with applicable rules in ISO/IEC 15944-4 and ISO/IEC 15944-5 but this document does so from a PPP requirements and PbD perspective. This clause summarizes the "privacy" collaboration space.

7.2 Collaboration space: Role of consumer (as individual), vendor and regulator

The collaboration space, introduced and defined in ISO/IEC 15944-4, focuses on collaboration space from an internal constraints perspective only. ISO/IEC 15944-5 focuses on adding external constraints from the perspective of the requirements of jurisdictional domains. They are modelled by adding: (1) a regulator" (as already introduced and provided for in ISO/IEC 15944-1:2011, 6.2.6; and, (2) the three sub-types of Person (see ISO/IEC 15944-1:2011, 6.2.7).

Where a Person is acting as an individual, the external constraints identified in 5.4 can be required. Thus, when modeling a scenario, two possible approaches can be used. In the first, it will be necessary to identify different scenario components in the model when addressing scenarios which involve privacy protection from those that do not. In the second, the privacy constraints are required to be included in the model with an option to switch them off for the scenarios where privacy requirements are absent. Either approach is valid.

Another minimum external constraint that is taken into account in business transactions is that commonly known as "consumer protection". The sole purpose of this clause is to ensure that when one uses this document to model business transactions or parts of business transactions as scenarios and scenario components, one does note under "external constraints" whether or not the scenario and/or the scenario component supports external constraints of a consumer protection nature.

There may be more than one role fulfilled by the regulator (or regulators) in the business transaction, since the regulator may act to supervise that the information constraint(s) have been applied, or can act to provide an anonymous or pseudonymous identity for one or more of the parties to the business transaction (which can include the regulator). The regulator is the source of external constraints in a privacy collaboration space (PCS).

The overall business transaction being modelled (as a scenario or scenario component) involves: (1) a "buyer" who is an individual; and, (2) the jurisdictional domain(s) involved having or exerting external constraints of a privacy protection nature.

This is illustrated in Figure 4 (as adapted from Figure 5 in ISO/IEC 15944-5). It is noted that in some business transactions the seller as well as the buyer can both be making use of an agent or a third-party supplier for the purpose(s) of concluding a business transaction.

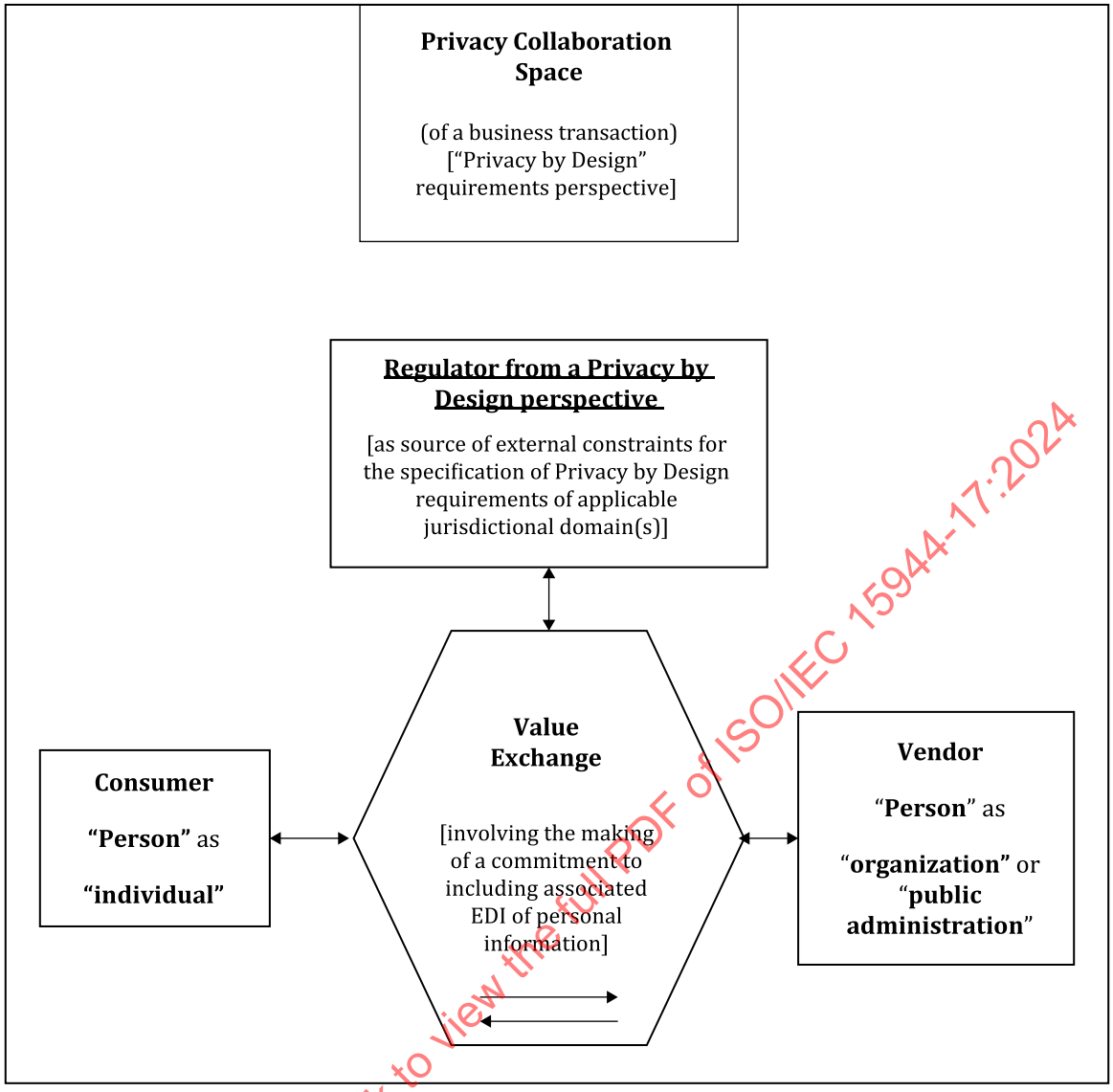

Figure 4 — Privacy collaboration space (of a business transaction) including the role of a regulator

The rules stated in ISO/IEC 15944-8:2012, 6.3 apply to this document. (refer to Rule 38 in B.5)

Rule 034:

An organization shall ensure that any artificial intelligence, machine learning and/or data mining activities undertaken by itself (or via an agent or third party on its behalf) to automate business transaction decisions that impact an individual in the privacy collaboration space, shall be in compliance with applicable privacy protection requirements, and not involve any secondary use or any other use of personal information for which the individual concerned has not provided explicitly informed consent.

Rule 035:

An individual shall be able to challenge the organization's sole use of artificial intelligence, machine learning and/or data mining activities with respect to a business transaction and request human intervention[9][10].

A rule additional to ISO/IEC 15944-8:2012 and adapted from Rule 013 is:

Rule 036:

Except with the explicit informed consent of the individual, or as required by law, personal information collected in the privacy collaboration space (independent view) 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.

This means that in the privacy collaboration space, the personal information of the individual as the buyer in the business transaction collected by the seller in that business transaction, Enterprise #2, shall not be disclosed, i.e. communicated, to any other party(ies), Enterprise #1, unless so required for the actualization of that specific business transaction with the individual being fully informed of the same by the seller and having consented to. This is illustrated in Figures 5 and 6 REA – patterned compound sentence (Independent View)[5].

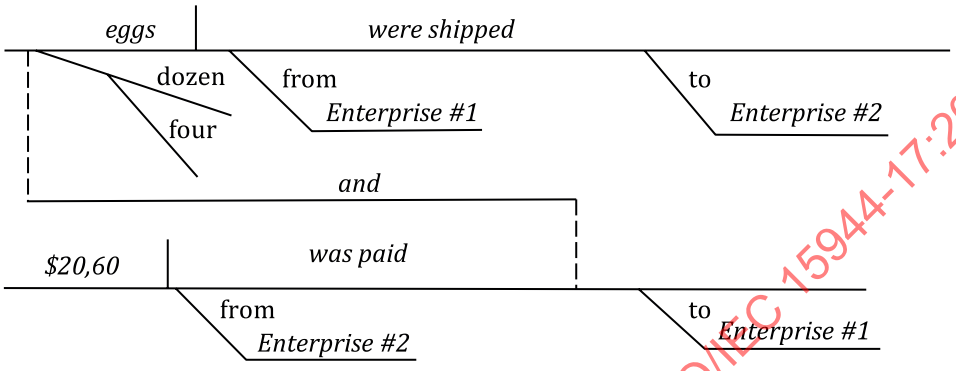

Figure 5 — Generalized collaboration space

Figure 6 takes the generalized model and adapts it in a privacy protection and Privacy by Design context. Further in REA, the use of "enterprise" is generic in nature and should be considered a synonym for "organization".

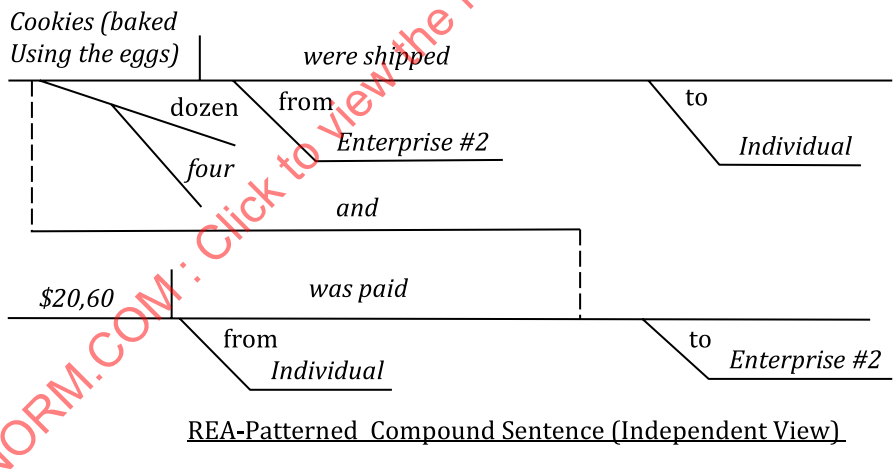

Figure 6 — collaboration space involving an individual and personal information

8 Ensuring that personal information is 'under the control of' the organization throughout its ILCM

8.1 Overview

Privacy by Design, having PPR embedded into the IT system and initiated in the collaboration space, extends securely throughout the entire lifecycle of the personal information involved. —Robust information life cycle management (ILCM) measures are essential to ensuring the implementation and compliance by any organization of applicable privacy protection requirements as these apply to any of its "*organization Persons*"

as well as any of its actual or potential "*customers*". This ensures that all personal information are securely retained, and then securely destroyed at the end of the ILCM process, in a timely fashion.

The significance of ILCM to PbD is the 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, including expungement, in compliance with applicable information law requirements.

8.2 Rules governing the specification of ILCM aspects of personal information

The rules stated in ISO/IEC 15944-12:2020, 6.2 that reference a high-level set of generic ILCM principles which integrate and are embedded in the eleven (11) fundamental privacy protection principles, rules, guidelines and associated normative text apply to this document.

Rule 037:

Privacy protection requirements continue to apply to the personal information of an individual after his/her death and will follow those of the jurisdictional domain.

Guideline 037G1:

In addition, from a business transaction perspective, there may be some continuity in privacy protection requirements, [e.g. those pertaining to temporal aspects of post-actualization aspects of an instantiated business transaction, (e.g. health care matters, warranties on products, service contracts, rights, including IP), etc.]. Instantiated business transactions may require personal information to be retained and continue to be protected following the death of the individual.

NOTE 1 This can also include a settlement of wills, probate, investments, etc., pertaining to that individual once proved deceased.

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

NOTE 3 Instantiated business transactions can require personal information to be retained and continue to be protected following the death of an individual, (e.g., many credit card agreements exist after the death of the credit card holder).

8.3 Implementing "under the control of" and accountability[6)]

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 PIC can 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 role of a PIC can l be carried out by a single organizational Person.

The information life cycle management (ILCM) is focused on implementation aspects as well as serving as a bridge between the BOV and FSV, thereby significant to Privacy by Design. 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.

It is not uncommon that in the "actualization" of a business transaction that the seller may well use one or more "agents", now commonly known as "outsourcing". The role of such agents may range from a simple transport delivery role to one including the undertaking of many other business operational functions which a seller may delegate to an agent. In some cases, it is also a third party, i.e., where the use of such a designated third party is either mandated by the rules of the applicable jurisdictional domain in which the business transaction is taking place, and/or the seller and buyer. At the same time, it is also not uncommon that the actualization of the business transaction involves the use of third parties. The use and role of third

6) This Clause and its rules complement those of ISO/IEC 15944-8:2017, 5.3.2, which applies. See further B.5.

parties may be mutually consented to by the buyer and seller, i.e., as part of modelling internal constraints, or be mandatory based on the requirements of an applicable regulator, i.e., as external constraints.

Privacy protection requirements which apply to the organization when providing a good, service and/or right to a buyer who is an individual often do not address directly the aspect of delegates (subcontractors) of role or functions in a business transaction delegated to an agent or third party. Commonly, the organization acting as the seller, i.e., as primary party, remains responsible and accountable for ensuring that privacy protection requirements are complied with for that business transaction regardless of how or where it is delivered.

The rules stated in ISO/IEC 15944-12:2020, Clauses 7 and 10 apply to this document.

Rule 038:

The use of agents and/or third parties by a seller in a business transaction to an organization or public administration (which has personal information under its control) shall not access or use such personal information processed as part of its services offering to that organization, unless it has a formal contractual arrangement to do so, in compliance with applicable privacy protection requirements.

Guideline 038G1:

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

Guideline 038G2:

It is presumed that when an organization "A" merges with, or is acquired by another organization "B", that the privacy protection requirements applicable to personal information under the control of organization "A" continue to apply and be enforced.

Guideline 038G3:

It is also assumed the personal information under the control of organization "A" remains under its control and that a merger with or acquisition by organization "B" does not allow organization "B" to access and/or use personal information held by organization "A" without the express and informed consent of the individuals whose personal information is/was organization "A".

9 Conformance statement[7)]

9.1 Overview

The first two types of conformance statements presented in Clause 9 are at the most primitive level only. More detailed conformance statement(s) with associated rules and procedures, including those pertaining to verification are expected to be developed either as Addendum(s) to this edition or as part of the development of another edition for this document.

Clause 9 is modelled on that found in ISO/IEC 14662:2010, Clause 6.

There are two different categories of conformance statements for this document; namely:

a) Category A – ISO/IEC 14662 Open-edi Reference Model; and, ISO/IEC 15944 compliance; and,

b) Category B – ISO/IEC 15944-17 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 this document 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.

7) Similar to that of, ISO/IEC 15944-8:2012, Clause 13 but with added sub-clauses re: conformance statement for "agent", "third party", and "regulator".

In addition, there are conformance statements for use by "agents" and "third parties". See further 9.4.

9.2 Conformance to the ISO/IEC 14662 Open-edi Reference Model and the multipart ISO/IEC 15944 eBusiness standard

Rule:039:

This clear commitment at the highest level within an organization also shall apply to any electronic data interchange (EDI) of personal information of individuals as in their role as a consumer in the provision of a good, service, and/or right by the organization

Rule 040:

Any user/implementer conformance statement of this nature shall state: (a) that it is conformant to the BOV class of standards of ISO/IEC 14662; (b) the list of the basic concepts of the ISO/IEC Open-edi Reference Model and ISO/IEC eBusiness (BOV standards) as stated in the ISO/IEC 15944-7 eBusiness Vocabulary; and, (c) whether or not it has any Open-edi compliant scenarios and scenario components registered using ISO/IEC 15944-2.

9.3 Conformance to ISO/IEC 15944-17

Rule 041:

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 PbD requirements as stated in ISO/IEC 15944-17 definitions, its concepts, rules, guidelines and related requirements".

9.4 Conformance by agents and third parties to ISO/IEC 15944-17

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 that such personal information maintained under the control of the organization acting in the role of seller, including the organizations' IT Systems (and related DMAs). Where and when a (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 15944-17.

Rule 042

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 that 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 PbD requirements as stated as in ISO/IEC 15944-17 definitions, its concepts, rules, and related requirements. This includes organization "XYZ" having a designated role/function of privacy protection officer (PPO) and of personal information controller (PIC).as an organization person(s)".*

Annex A
(normative)

Consolidated controlled vocabulary definitions and associated terms, as human interface equivalents (HIEs), with cultural adaptability: English and French language equivalency in an IT standardization context

A.1 Purpose

All parts of the ISO/IEC 15944 series of eBusiness standards maximize the use of existing standards, where and whenever possible, and in particular relevant and applicable existing terms and definitions of concepts as found existing ISO/IEC, ISO, or IEC existing standards. They are re-used either "as is" or as "adapted". These are many examples of the application of this rule found in Clause 3.

In addition, since the inception of the development multipart ISO/IEC 15944 eBusiness standard, back in 2000, the need for unambiguous definitions was recognized to minimize possible ambiguities in the same, as well as, to facilitate their implementations by users in an international and multilingual eBusiness context.

A.2 Maximizing unambiguity and quality control

In order to maximize unambiguity and ensure necessary quality in the ISO/IEC 15944 series of eBusiness standards, as well to facilitate multilingual and international interoperability of key eBusiness definitions and their associated terms, the concept and definition of "human interface equivalencies (HIEs) was developed for several reasons, the four primary reasons being that,

a) international standards development, by its very nature, focuses on identifying new issues, needs and resolving them. This includes identification of new concepts, developing an "international standard" definition for the same, and then deciding on the label, i.e. term, to be assigned to the definition of this new concept. Here it is most likely that the "term" assigned to the definition of the new concept will be, as what is known in terminology work as an invented, i.e. "coined" term (see ISO/IEC 15944-7:2009, 5.3.2. This means that such new English language "coined" terms in an international standard are not found in exiting English language dictionaries, i.e. they are first introduced into the English language via an ISO/IEC (as well as ISO or IEC) standard.

   In order, to ensure that there is no ambiguity in the definition of a new concept. Thus, it is very likely that the introduction of these new concepts, the development of their definitions and assignment of a label, i.e., "term" to the same in an international standard will not have a semantic equivalent in another language. As such it is unlikely that equivalent translation exists. Instead, one needs to view this as a challenge of developing a human interface equivalent (HIE) in another language.

   As such, it is the approach of this document and other parts of ISO/IEC 15944, as well as ISO/IEC 14662 to use HIEs in English and French in the IT standardization context.

b) Where the use any part ISO/IEC 15944 of the multipart series of eBusiness standard (as well as any other ISO/IEC. ISO, IEC, ITU, etc.), involves, or impacts, an individual as the "buyer" of any good, service and/or right of any nature (including those provided to individuals by private or public sector organizations, including public administrations), then international, regional and national public policy requirements of a legal/and regulatory requirements apply.

   The most common of the international legal/regulatory requirement of a "public policy" nature already identified and supported in the multipart series of ISO/IEC 15944 series of eBusiness standards as

defined set of rights of an include "consumer protection, privacy protection, individual accessibility, human rights[8], etc. [9].

c) ISO/IEC JTC1 has "cultural adaptability" as the third strategic direction which all standards development should support, where applicable. The other two strategic directions of ISO/IEC JTC1 standards development are "portability" and "interoperability". Here it is noted that the ISO Technical Management Board (TMB) has permitted ISO/IEC JTC1 to issue its standards in the English language only, instead of in the three official languages ISO, i.e., English, French and Russian[10].

Therefore, when a new concept, its definition and associated term is developed, it is necessary at the same time to develop HIEs for the same in one or more other languages. This approach,

— adds a level of "quality control check" as developing an equivalency in another language identifies ambiguities in the source language;

— recognizes that in languages other than English, specifying the grammatical gender of the term is essential (since the same word, i.e., character string, may well 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 eBusiness standards world-wide, especially users of this document who include various industry sectors, different legal perspectives, policy makers and consumer representatives, other standard developers, IT hardware and service providers, etc.; and,

— takes an IT-enabled approach which promotes interoperability from both IT interface and human interface perspective (see ISO/IEC 15944-5). An essential aspect of this approach is to assign and use the unique and unambiguous composite identifier of each term/definition pair as the ID code with which are associated multiple bilingual/multilingual semantically HIE representations.

d) In 2006, the United Nations adopted the *UN Convention of rights of persons with disabilities (CRPD)*[11]. It is noted that the concept and definition of HIE (developed as part of the 1st edition of ISO/IEC 15944-2:2006 was developed in support of the UN CRPD. It is noted that ISO/IEC JTC1/SC36 developed ISO/IEC 20016-1[15]. Significant normative elements in the development of the ISO/IEC 20016-1, i.e. definitions, rules, etc., are based on ISO/IEC 15944 eBusiness standards.

e) Here the development by ISO/IEC JTC1/32 with the introduction of the concept and controlled vocabulary of ISO/IEC 15944 eBusiness standards.

A.3 Role and importance of ISO/IEC 15944-7 — eBusiness vocabulary in support of facilitating HIE approach

Based on the need to maximize unambiguity and quality control in the development of an HIE approach to entries in Clause 3, ISO/IEC 15944-7 was developed to capture in a formalized manner:

— applicable international standards in the fields of terminology and vocabulary (These are primarily those of ISO TC 37 and ISO TC 46); and,

8) Article 19, of the UN Charter of Universal Declaration of Human Rights specify what these are. See further https://www.un.org/en/about-us/universal-declaration-of-human-rights

9) These important legal/regulatory requirements as public policy rights of an individual are introduced, explained, fully supported and defined in ISO/IEC 15944-5.

10) A primary reason here is that many ISO/IEC JTC1 standards introduce an artificial language, (e.g., a i.e., "programming language", a "database language", etc.) and thus do not use a "natural", i.e., human, language.

11) Currently, all countries who are P-members of ISO/IEC JTC1 are also signatories to the CRPD.
The development of this standard had as its primary requirement to implement CRDP requirements in an eLearning context. In addition, its development was based on the assumption that a "requirements pertaining to a "learning transaction" were very similar to those already addressed in a "business transaction", i.e., including the need to identify where in a learning transaction the "buyer", i.e. "learner", in an JTC1/SC36 eLearning standards context was an "individual" or not (e.g. "organizations" providing eLearning services to other).
ISO/IEC 20016-1 was also found to be a base foundational "Framework" standards freely available ISO/IEC JTC standard.

— apply them in a practical, IT-enabled and cost-efficient manner in a multilingual eBusiness requirements context. (initially based on the lessons learned in the development of ISO/IEC 14662 and 1st editions of ISO/IEC 15944-1, ISO/IEC 15944-2, ISO/IEC 15944-4, ISO/IEC 15944-5 and ISO/IEC 15944-6)

The results are formalized in ISO/IEC 15944-7:2009, Clause 5, and in particular its subclause 5.2.

An important result is that when and wherever in the development a new Part of ISO/IEC 15944 involved the identification of a new concept and the development of a definition (as well as assignment of a term for a new concept), the rules found in Clause 5 of ISO/IEC 15944-7 apply, including the requirements to provide an HIE in at least one other language.

This requirement has been met in the development of this document. For the English and French HIEs in this document, see ISO/IEC 15944-7:2009, Annex D.

ISO/IEC 15944-7, a publicly available standard at the ISO publicly available standard website[12], provides rules and procedures for creating and maintaining a (consolidated) "controlled vocabulary" and basically its Annex D provides a list of HIEs that provides the minimum level of unambiguity in ISO/IEC 15944 eBusiness standards as stated in A.1.

A.4 List of terms and definition with cultural adaptability: English and French language equivalency in the IT standardization context

For English and French HIEs in this document, see ISO/IEC 15944-7:2009, Annex D.

12) See https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Annex B
(normative)

Consolidated set of rules in existing Parts of ISO/IEC 15944 of particular relevance to PbD as external constraints on business transactions which apply to personal information (PI) in an EDI and collaboration space context

B.1 Overview

This document already makes extensive use of relevant rules and guidelines as found in referenced Clauses in ISO/IEC 15944-1 and adapts them in a PbD requirements context. Similarly, relevant rules and guidelines found in ISO/IEC 14662, ISO/IEC 15944-5, ISO/IEC 15944-8, ISO/IEC 15944-12 have been adapted or serve as the basis for rules[13)] of this nature required to support PbD requirements.

The purpose of Annex B is to provide a consolidated presentation of all the rules which are relevant 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 by Design. Jurisdictional domains are the primary source of external constraints. The existing parts of ISO/IEC 15944 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 current editions of Parts of ISO/IEC 15944 identified in the matrixes below.

B.2 Organization of Annex B: Consolidated list in matrix form

The rules and associated references are presented in matrix form as Table B.2, Table B.3, Table B.4 and Table B.5. The rules are presented in the numeric order in which they are presented in ISO/IEC 15944-1, ISO/IEC 15944-5, ISO/IEC 15944-8 and ISO/IEC 15944-12. The columns in the matrix are given in Table B.1.

Table B.1 — Columns in Table B.2, Table B.3, Table B.4 and Table B.5

Col. No	Use
1	Number of Rule as per Part of ISO/IEC 15944 referenced in the Annex B subclause.
2	Clause ID 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 ISO/IEC 15944. All Parts of ISO/IEC 15944 are ISO "freely available standards".

13) ISO/IEC 15944-16 provides a consolidated set of rules and guidelines found in ISO/IEC 15944.

Table B.2 — Consolidated lists of rules and associated guidelines in ISO/IEC 15944-1 supporting PbD

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 can allow a Person to use the same persona and its associated identification schema (including resulting identifiers), while others can 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, can 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.
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.
49	6.5.1	Open-edi scenarios and Information Bundles shall therefore be capable of reflecting constraints to be applied which can be as a result of: (a) commitments among parties, i.e., as internal constraints; and, (b) external constraints.
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.
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.

Table B.2 *(continued)*

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
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.
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 can be associated with an SC ID, (e.g., as "aliases").

Table B.3 — Consolidated lists of rules and associated guidelines in ISO/IEC 15944-5 supporting PbD

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 can specify and require the business transaction to be enacted in a specified jurisdictional domain
004	5.2.3	Within a particular jurisdictional domain, Referencing a specific act or regulation can be required as well as requiring 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 can specify the "explicitly shared goal" of a business transaction as a whole.

Table B.3 *(continued)*

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
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.
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/(Terminology) code set 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 can 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 can have either one or more official languages and, if not, can 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 can 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.

Table B.3 *(continued)*

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
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.
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 it 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 can 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.
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.

Table B.4 — Consolidated lists of rules and associated guidelines in ISO/IEC 15944-8 supporting PbD

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
001	5.2	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
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.

Table B.4 *(continued)*

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
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.
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 fulfillment 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.

Table B.4 *(continued)*

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
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.
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 can 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:

Table B.4 *(continued)*

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
		1) shall not be communicated with other parties; 2) can be communicated to other parties but with restrictions; or, 3) can be communicated to other parties with no restrictions.
037	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, i.e., the need to ensure the provision of a tag(s) to note that the personal information is subject to mandatory disclosure is: 1) the actual information; 2) anonymous information that represents the actual information; or, 3) pseudonyms that represent the actual information.
038	6.3	For any business transaction (or part thereof) which involves external constraint(s) of a privacy protection nature, the Open-edi model shall include: 1) the Person in the role of buyer as an individual; 2) the role of the regulator(s) representing the source of privacy protection requirements for modelling as part of a scenario and scenario component; 3) the role of the regulator(s) providing proof of identity of the individual without necessarily disclosing the actual identity of the individual.
040	7.2.1	Where the buyer in a business transaction is an individual, external constraints of a privacy protection nature of jurisdictional domains apply and shall be supported in applicable business scenarios and scenario components.
042	7.2.1	Where the buyer in a business transaction is an individual, external constraint of a privacy protection nature of jurisdictional domains apply and shall be supported in applicable business scenarios and scenario components.
043	7.2.1	A seller shall ascertain, at the identification phase in the process leading to a business transaction, whether or not the buyer is an individual (not someone as organization Person buying on behalf of an organization or public administration).
044	7.2.2	A common set of external constraints of a jurisdictional domain on a business transaction, where the buyer is an individual, are those of a consumer protection nature. As such, any business transaction involving an "individual" in the role of buyer shall be structured to be able to support applicable "consumer protection" requirements.
045	7.2.2	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.
048	7.2.5	Privacy protection requirements apply only to a natural person, i.e., human being, acting in the role of an individual.
049	8.2	The primary set of generic principles and rules, as well as associated concepts and their definitions governing the creation, recognition, use, management of identities of a Person as stated in ISO/IEC 15944-1:2011, 6.1.4 and 6.2.2 apply here.
055	8.3	Where a Registration Authority (RA) administers more than one Registration Schema which involves individuals (and their associated personal information), the RA shall not use personal information provided by the individual under one Registration Schema (RS) in another RS of the RA without the explicit consent of the individual concerned unless required by applicable law.
056	8.4	The individual identity, i.e., the persona and the associated identifier, used by an individual in a business transaction, shall be capable of being prescribed depending on the context and goal of the business transaction.

Table B.4 *(continued)*

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
057	8.4	A specific individual identity (ii) established by a Registration Authority, (organization or public administration), should not be used for any purpose other than that for which it was created, without the express and explicit consent of the individual.
062	9.2	The Clause 8.4 "Rules for the specification of Open-edi roles and role attributes", as stated in ISO/IEC 15944-1 are mandatory where the business transaction involves an individual as a buyer.
063	9.2	Prior to the start of the actualization phase of a business transaction, a seller shall ascertain whether or not the Person acting as a buyer is doing so in its capacity or status as an individual (rather than as an organization Person or other roles of a Person).
064	9.2	Where the buyer in a business transaction is an individual, the buyer shall: 1) ensure that privacy protection requirements as stated in ISO/IEC 15944-8 are applied; and, 2) ascertain whether or not other external constraints apply with respect the individual meeting specified criteria of the applicable jurisdictional domain(s) in qualifying for the role of buyer with respect to the good, service, and/or right which is the goal of the business transaction.
065	9.2	When the identification and negotiation phase of a business transaction does not result in its actualization and the prospective buyer is an individual, the seller (or regulator) shall delete all personal information on that individual gathered at that time.
066	9.3	The rules in ISO/IEC 15944-5:2008, 6.6.2.3 apply.
067	9.3	Where the buyer in a business transaction is an individual, the seller shall inform itself as to whether external constraints apply which require the individual to use a legally recognized name (LRN) as its persona, as well as the nature of the Source Authority for such as LRN.
068	9.4	The rules governing the truncation of a persona, as stated in ISO 7501 series, ISO 7812 series, and ISO/IEC 15944-1, apply to ISO/IEC 15944-8
069	9.4	Where external constraints on a business transaction require an individual as a (potential) buyer using a legally recognized name (LRN) as the persona for that individual, the seller shall specify the types of LRNs permitted to be used by the individual.
070	9.4	Where external constraints on a business transaction require that the personae of the individual be provided using a specified language or character set which is different from the language which the individual uses for his/her persona (or is his/her birth name), then the transliteration rules of the ISO 7501 series shall apply.
071	9.5	Identification of a Person as buyer in a business transaction is not always necessary in (electronic) business transaction involving the seller knowing whether or not the buyer is an individual.
072	9.5	Unless explicitly proscribed, (not allowed) by external constraints of the relevant jurisdictional domain applicable to the specified goal of the business transaction to be entered into, an individual as buyer many decide to remain anonymous in that business transaction, and no personal information on the individual is maintained by the seller or other parties
073	9.6	Unless explicitly proscribed (not allowed) by external constraints of the relevant jurisdictional domain applicable to the specified goal of the business transaction to be entered into, an individual, as a buyer, can decide to use a pseudonym in that business transaction, and no personal information on the individual in particular its name remains private
078	10.3	During the identification phase, the seller shall ascertain whether or not the buyer is an individual, and if so, inform the individual of the privacy policy of the seller.
079	10.4	Where the buyer is an individual, the end of the negotiation phase shall include the explicit consent of the individual for provision of its personal information, as identified and specified, as well as the specification of the information life cycle management (ILCM) and EDI aspects of such personal information, as stated in 5.3 "Privacy Principles".

Table B.4 *(continued)*

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
080	10.5	Where the buyer is an individual, the seller shall ensure and have in place procedures and mechanisms to support both the generic privacy protection requirements as: (1) found in ISO/IEC 15944-8 and stated in its rules and guidelines; and, (2) as well as those resulting from the negotiation phase, i.e., as negotiated between the seller and the individual as buyer.
081	10.6	A buyer (and its agent(s)) or third party (or any other party to the business transaction), shall not retain any personal information on the individual as the buyer for any time longer than is consented to by the individual for post-actualization purposes unless external constraints of the applicable jurisdictional domain requires retention of such personal information for a longer period.
082	10.6	Where the buyer gifts the product to another individual, and the terms of the purchase allow the recipient individual to assume the warranty, extended service contract, etc., the seller shall ensure that such a recipient individual is fully informed of its privacy protection rights, including the record retention requirements.
083	11.2	Each instantiated business transaction involving an individual as a buyer shall have a business transaction identifier (BTI) assigned by the seller or the regulator.
084	11.2	Where an individual as a buyer in a business transaction decides to be anonymous (as permitted by the external constraints of the applicable jurisdictional domain), the business transaction identifier (BTI) serves as the sole identifier.
085	11.2	Where the business transaction is of the nature of a regulatory business transaction (RBT) and the rules governing the RBT permit an individual to be a buyer, such rules shall explicitly state and define the associated personal information in conformance with ISO/IEC 15944-8
086	11.3	The rules governing state changes of recorded information (Clause 6.6.4.3 "State Changes" in ISO/IEC 15944-5) apply to any business transaction involving an individual as a buyer.
087	11.4	The rules governing the specification of records retention requirements are stated in ISO/IEC 15944-1:2011, 8.5.2.8 and 8.5.2.9 and in ISO/IEC 15944-5:2008, 6.6.4.2 and are mandatory to any business transaction involving an individual as a buyer, i.e., to all resulting information.
088	11.4	Where the buyer is an individual, the seller shall inform the buyer of all records retention aspects whether of internal or external information, with respect to the sets of recorded information (SRIs) pertaining to the personal information forming part of the business transaction, and in particular those pertaining to the post-actualization phase.
089	11.5	The rules governing temporal referencing as stated in Clause 6.6.4.5 "Date/time referencing" as stated in ISO/IEC 15944-5 apply when the individual is a buyer in a business transaction and thus privacy protection requirements apply.
090	11.5	Unless otherwise specified and agreed to by the individual as buyer in a business transaction, the common temporal referencing schema of the jurisdictional domain of the individual applies.
091	11.5	The temporal referencing schema governing the business transaction where the buyer is an individual shall also be used to ensure deletion of sets of personal information as required by privacy protection requirements.
093	12.2	It is equally important in scoping an Open-edi scenario (OeS) which allows for an individual as buyer in a business transaction to note whether this is an adaptation of an existing "generic" OeS or a new OeS. It is understood that (a) most of the Open-edi scenarios will be and are modelled at the Person level; and, (b) that many of these need only minor modifications in their modelling of such scenarios to incorporate privacy protection requirements.
F-001	F.1	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.

Table B.4 *(continued)*

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
F-002	F.2.2	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 data management and interchange required to comply with privacy protection requirements
F-004	F.3	Where an individual is a buyer to a business transaction, the seller shall specify who is responsible for the retention of any (combination of) set(s) of recorded information during the negotiation phase and no later than at the actualization phase in accordance with privacy protection requirements.
F-005	F.3	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 destruction requirements).
F-006	F.3	Where an individual is a buyer to a business transaction, the seller shall specify the "retention trigger" activating records retention requirements in accordance with privacy protection requirements of the applicable jurisdictional domain(s).
F-007	F.4	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.

Table B.5 — Consolidated lists of rules and associated guidelines in ISO/IEC 15944-12 supporting PbD

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
004	5.4	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.
005	5.5	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.
006	5.7	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
007	5.8	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).
008	5.8	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.
009	6.2.1	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].